INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

The Standard of Good Practice for Information Security

2007

Information for Non-ISF Members

The Standard of Good Practice for Information Security (the Standard) has been produced by the Information Security Forum (ISF), an international association of over 300 leading organisations which fund and co-operate in the development of a practical research programme in information security. During the last 18 years the ISF has spent more than US$100 million providing authoritative material to its Members. The ISF's work represents the most comprehensive and integrated set of material anywhere in the world in the area of information risk management.

The Standard of Good Practice is a key deliverable from the ISF's extensive work programme. It has been developed and enhanced over a number of years and has benefited from the results of the many projects run by the ISF.

As the ISF is a membership organisation, ISF reports are normally for the exclusive use of ISF Members. However, the ISF has made *The Standard of Good Practice* available to non-Members with the objectives of:

- promoting good practice in information security in all organisations worldwide
- helping organisations which are not Members of the ISF to improve their level of security and to reduce their information risk to an acceptable level
- assisting in the development of standards that are practical, focused on the right areas, and effective in reducing information risk.

The Standard has been developed using a proven methodology to produce the international benchmark for information security. The Standard is updated regularly, refining proven practices and addressing 'hot topics'.

The ISF runs a comprehensive *Information Security Status Survey* that enables Members to gain a clear picture of their organisation's performance across all aspects of information security. The Survey provides a practical, automated tool with which a Member organisation can measure the effectiveness of their information security arrangements, compare them with those of other leading organisations, and assess how well they are performing against *The Standard of Good Practice*.

For information about the ISF please e-mail us at isfinfo@securityforum.org or visit our website at www.securityforum.org

---

This document has been produced with care and to the best of our ability. However, both the Information Security Forum and the Information Security Forum Limited accept no responsibility for any problems or incidents arising from its use.

We take great care to minimise the impact on the environment in the paper we use. The paper we have used in this document is FSC* certified and manufactured at an ISO14001** accredited mill.

*FSC – Forest Stewardship Council. This ensures there is an audited chain of custody from the tree in the well managed forest through to the finished document in the printing factory.

**ISO14001 – A pattern of control for an environmental management system against which an organisation can be accredited by a third party.

Contents

Introduction

Provides a brief introduction to the Standard, explains what the Standard consists of, and highlights the key benefits of using the Standard.

Principles and Objectives

Explains the terms 'principle' and 'objective', and brings together each principle and objective used in the Standard.

Topics Matrix

Groups individual sections of the Standard under similar topic headings in a simple to use alphabetic reference table.

The Standard of Good Practice

SM Security Management (enterprise-wide)

Covers topics relating to high-level direction for information security, arrangements for information security across the organisation, and establishing a secure environment.

CB Critical Business Applications

Covers topics relating to requirements for securing business applications, identifying information risks and determining the level of protection required to keep information risks within acceptable limits.

CI Computer Installations

Covers topics relating to the design and configuration of computer systems, management activities required to establish a secure computer installation and maintain service continuity.

NW Networks

Covers topics relating to network design and implementation, management activities required to run and manage secure networks, including local and wide area networks, and voice communication networks.

SD Systems Development

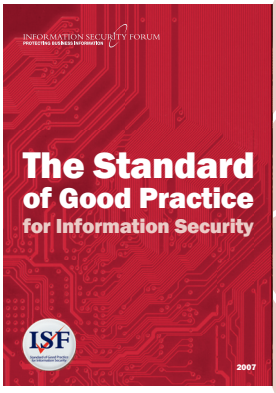
Covers topics relating to the application of information security during all stages of systems development, including design, build, testing and implementation.

UE End User Environment

Covers topics relating to local security management, protecting corporate and desktop applications, and securing portable computing devices.

Index

Provides a comprehensive list of terms used within the Standard, and references each statement of good practice that uses each particular term.



1. Development of the Standard

- Based on the output of an extensive work programme
- Builds upon major information security-related standards
- Incorporates the views and experiences of over 300 leading international organisations
- Continually updated, at least every two years.

2. Contents of the Standard

- Covers an extensive range of information security topics
- Provides coverage of the latest 'hot topics' in information security
- Includes end user computing (eg spreadsheets)
- Aligned with major information security-related standards.

3. Presentation of the Standard

- Presents a comprehensive set of security-specific controls using clear and unambiguous text
- Available in printed form as a comprehensive reference document for quick reference
- Presented in several electronic formats including PDF, Word, Excel and XML, to support different organisation's needs
- Modular format provides ability to focus on key areas
- Includes a topics matrix and comprehensive index to help look up and locate essential topics quickly.

4. Application of the Standard

- Can replace, augment or complement an organisation's internal standards
- Linked to a powerful benchmarking tool
- Can be used standalone or in conjunction with other ISF tools and methodologies.

Figure 1: Features of the Standard of Good Practice

The range of features of the Standard are examined in the accompanying report entitled ***Making the most of the Standard***, which is available from the ISF's Member-only extranet (MX²), and also from the ISF's public website ***www.securityforum.org***.

Introduction to the Standard

About The Standard of Good Practice

The Standard of Good Practice for Information Security (the Standard) is the foremost authority on information security. It addresses information security from a business perspective, providing a practical basis for assessing an organisation's information security arrangements.

The Standard contains a broad range of features (as shown in ***Figure 1***), covering the entire spectrum of arrangements that need to be made to keep the business risks associated with information systems within acceptable limits. As a result, it is a major tool for improving the quality and efficiency of information security controls applied by an organisation.

The Standard represents part of the ISF's information risk management suite of products and is based on a wealth of material, in-depth research, and the extensive knowledge and practical experience of ISF Members worldwide. It is updated at least every two years in order to:

- respond to the needs of leading international organisations
- refine areas of best practice for information security
- reflect the most up-to-date thinking in information security
- remain aligned with other information security-related standards, such as ISO 27002 (17799) and COBIT v4.1
- include information on the latest 'hot topics'.

Basis for the Standard

Since the first release of the Standard in 1996, it has been developed and enhanced every two years, using a proven methodology, to produce ***the*** international standard for information security.

Development of the Standard is based on the results of three main groups of activities (as shown in ***Figure 2***).

An extensive work programme involving the expertise of a full-time ISF Management Team, that performs comprehensive research into hot topics in information security, produces reports, tools and methodologies, and maintains strategic projects such as the ISF's Information Risk Analysis Methodology (IRAM).

Analysis and integration of information security-related standards (eg ISO 27002 and COBIT v4.1), and legal and regulatory requirements (eg Sarbanes-Oxley Act 2002, Payment Card Industry (PCI) Data Security Standard, Basel II 1998, and the EU Directive on Data Protection).

The involvement of ISF Members, using techniques such as workshops, face-to-face meetings and interviews, and the results of the ISF's Information Security Status Survey.

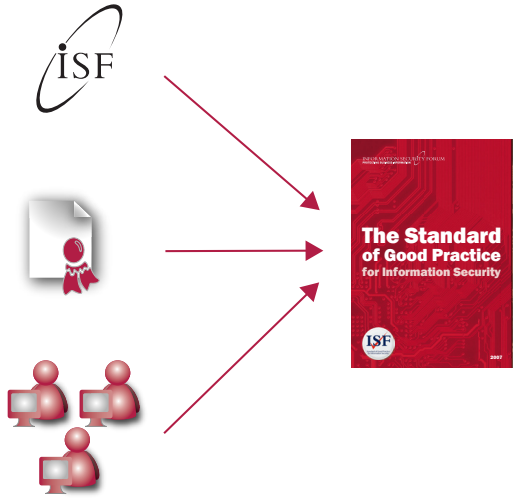


Figure 2: Basis for the Standard of Good Practice

Target audience

The Standard is aimed at major national and international organisations that recognise information security as a key business issue. However, the Standard will also be of real, practical use to any type of organisation, such as a small- to medium-sized enterprise.

Good practice detailed in the Standard will typically be incorporated into an organisation's information security arrangements by a range of key individuals or third parties, including:

- **information security managers** or equivalent, responsible for promoting or implementing information security
- **business managers** responsible for running critical business applications and managing end user environments
- **IT managers** responsible for planning, developing, installing, running or maintaining key information systems or facilities
- **IT audit managers** responsible for conducting security audits of particular environments
- **outsource providers** responsible for managing IT facilities (eg computer installations and networks) on behalf of the organisation.

The Standard

Introduction

The Standard of Good Practice covers six distinct aspects of information security, each of which relates to a particular type of environment. It also includes additional material (eg topics matrix and index) to help Members locate information quickly and easily. Accordingly, this part of the Standard provides an:

- explanation and summary table of the six aspects of information security
- outline of the structure and layout of the aspects
- overview of the principles and objectives, topics matrix and index.

The six aspects of information security

The Standard focuses on how information security supports an organisation's key business processes. These processes increasingly depend on IT-based business applications, many of which are critical to their success. Thus the aspect of security concerned with Critical Business Applications is central to the design of the Standard, as shown in ***Figure 3***.

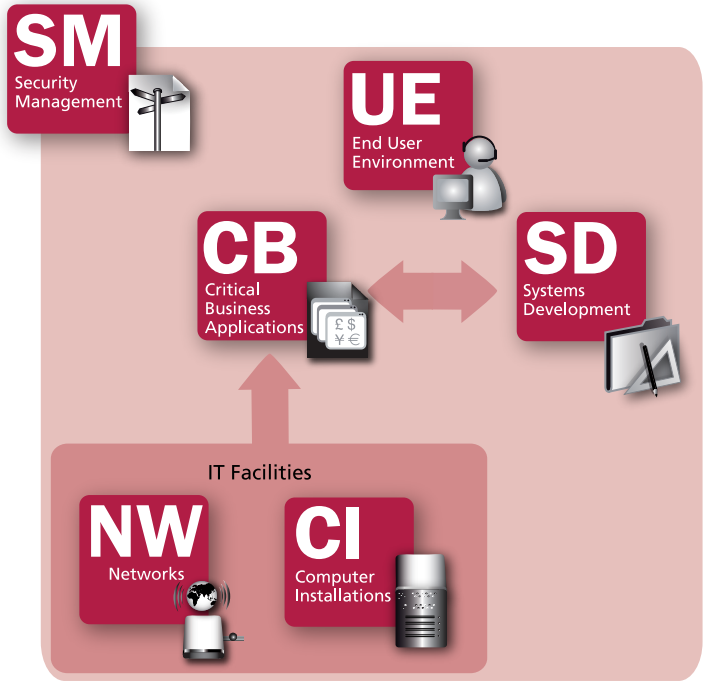


Figure 3: How aspects of the Standard interrelate

Computer Installations and ***Networks*** provide the underlying infrastructure on which the ***Critical Business Applications*** run. The ***End User Environment*** covers the arrangements associated with protecting corporate and desktop applications, which are used by individuals to process information, and support business processes. ***Systems Development*** deals with how new applications are created and ***Security Management*** addresses high-level direction and control.

A brief summary of each aspect can be found in ***Table 1*** on the following pages.

Table 1: Summary of The Standard of Good Practice

Aspect of security	Focus	Target audience
Security Management (enterprise-wide)	Security management at enterprise level.	The target audience of the SM aspect will typically include: • heads of information security functions • information security managers (or equivalent) • IT auditors.
Critical Business Applications	A business application that is critical to the success of the enterprise.	The target audience of the CB aspect will typically include: • owners of business applications • individuals in charge of business processes that are dependent on applications • systems integrators • technical staff, such as members of an application support team.
Computer Installations	A computer installation that supports one or more business applications.	The target audience of the CI aspect will typically include: • owners of computer installations • individuals in charge of running data centres • IT managers • third parties that operate computer installations for the organisation • IT auditors.
Networks	A network that supports one or more business applications.	The target audience of the NW aspect will typically include: • heads of specialist network functions • network managers • third parties that provide network services (eg Internet Service Providers) • IT auditors.
Systems Development	A systems development unit / department or a particular systems development project.	The target audience of the SD aspect will typically include: • heads of systems development functions • systems developers • IT auditors.
End User Environment	An environment (eg a business unit or department) in which individuals use corporate business applications and / or critical desktop applications to support business processes.	The target audience of the UE aspect will typically include: • business managers • individuals in the end user environment • local information security co-ordinators • information security managers (or equivalent).

Issues probed	Scope and coverage
The commitment provided by top management to promoting good information security practices across the enterprise, along with the allocation of appropriate resources.	Security management arrangements within: • a group of companies (or equivalent) • part of a group (eg subsidiary company or a business unit) • an individual organisation (eg a company or a government department).
The security requirements of the application and the arrangements made for identifying risks and keeping them within acceptable levels.	Critical business applications of any: • type (including transaction processing, process control, funds transfer, customer service and desktop applications) • size (eg applications supporting thousands of users or just a few).
How requirements for computer services are identified; and how the computers are set up and run in order to meet those requirements.	Computer installations: • of all sizes (including the largest mainframe, server-based systems and groups of PCs) • running in specialised environments (eg a purpose-built data centre) or in ordinary working environments (eg offices, factories and warehouses) • driven by any kind of operating system (eg IBM MVS, Digital VMS, Windows 2000 or UNIX).
How requirements for network services are identified; and how the networks are set up and run in order to meet those requirements.	Any type of communications network including: • wide area networks (WANs) or local area networks (LANs) • large scale (eg enterprise-wide) or small scale (eg an individual department or business unit) • those based on Internet technology such as intranets or extranets • voice, data or integrated.
How business requirements (including information security requirements) are identified; and how systems are designed and built to meet those requirements.	Development activity of all types, including: • projects of all sizes (ranging from many man-years to a few man-days) • those conducted by any type of developer (eg specialist unit / departments, outsourced or business users) • those based on tailor-made software or application packages.
The arrangements for user education and awareness; use of corporate business applications and critical desktop applications; and the protection of information associated with portable computing.	End user environments: • of any type (eg head office department, general business unit, factory floor or call centre) • of any size (eg several individuals to groups of more than one hundred) • that include individuals with varying degrees of IT skills and / or awareness of information security.

Intro

Structure and layout of the Standard

The six **aspects** within the Standard are composed of a number of **areas**, each covering a specific topic. An area is broken down further into **sections**, each of which contains a set of statements.

The overall structure of each aspect of the Standard is illustrated in ***Figure 4***, using the Security Management aspect as an example.

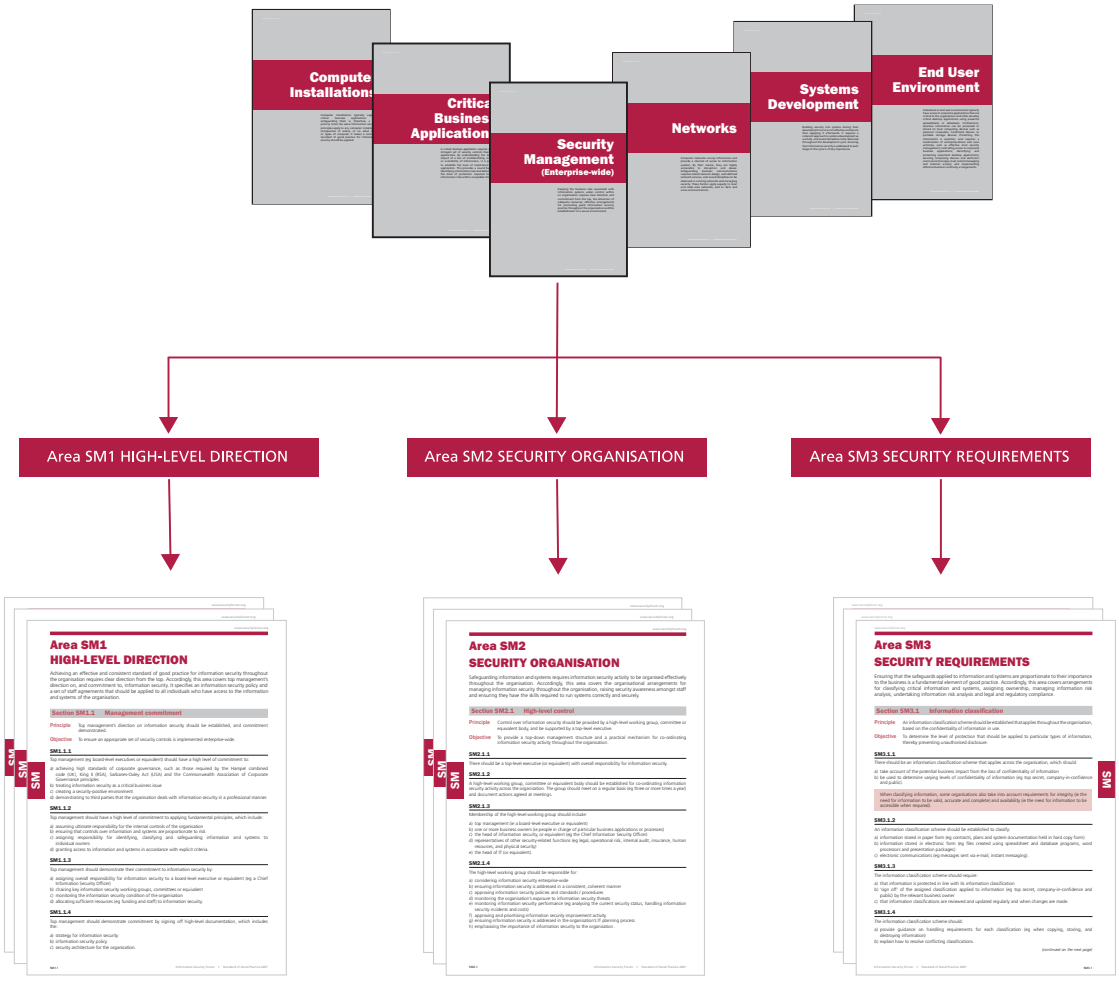
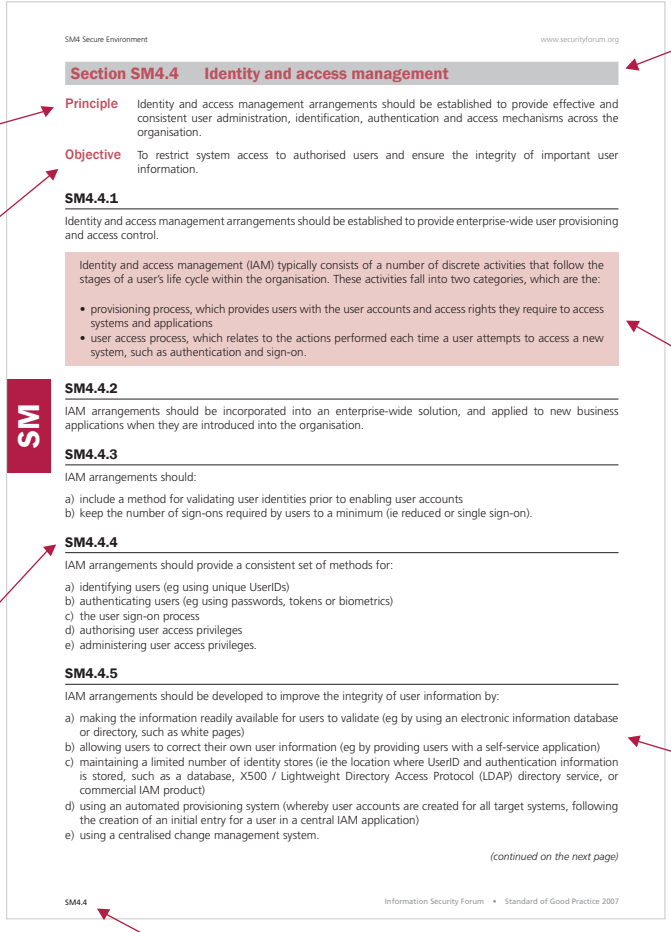


Figure 4: Structure of each aspect of the Standard

For each aspect and area presented in the Standard, a brief introduction is provided which encapsulates its importance and the main issues involved. Each of the sections is then set out as shown in ***Figure 5***.



SM4 Secure Environment www.securityforum.org

Section SM4.4 Identity and access management

Principle Identity and access management arrangements should be established to provide effective and consistent user administration, identification, authentication and access mechanisms across the organisation.

Objective To restrict system access to authorised users and ensure the integrity of important user information.

SM4.4.1

Identity and access management arrangements should be established to provide enterprise-wide user provisioning and access control.

Identity and access management (IAM) typically consists of a number of discrete activities that follow the stages of a user's life cycle within the organisation. These activities fall into two categories, which are the:

- provisioning process, which provides users with the user accounts and access rights they require to access systems and applications
- user access process, which relates to the actions performed each time a user attempts to access a new system, such as authentication and sign-on.

SM

SM4.4.2

IAM arrangements should be incorporated into an enterprise-wide solution, and applied to new business applications when they are introduced into the organisation.

SM4.4.3

IAM arrangements should:

a) include a method for validating user identities prior to enabling user accounts
b) keep the number of sign-ons required by users to a minimum (ie reduced or single sign-on).

SM4.4.4

IAM arrangements should provide a consistent set of methods for:

a) identifying users (eg using unique UserIDs)
b) authenticating users (eg using passwords, tokens or biometrics)
c) the user sign-on process
d) authorising user access privileges
e) administering user access privileges.

SM4.4.5

IAM arrangements should be developed to improve the integrity of user information by:

a) making the information readily available for users to validate (eg by using an electronic information database or directory, such as white pages)
b) allowing users to correct their own user information (eg by providing users with a self-service application)
c) maintaining a limited number of identity stores (ie the location where UserID and authentication information is stored, such as a database, X500 / Lightweight Directory Access Protocol (LDAP) directory service, or commercial IAM product)
d) using an automated provisioning system (whereby user accounts are created for all target systems, following the creation of an initial entry for a user in a central IAM application)
e) using a centralised change management system.

(continued on the next page)

Principle
A summary of the main set of security controls required (ie what controls need to be applied).

Objective
The purpose for applying a particular set of security controls (ie why controls need to be applied).

Aspect tab
Provides the reader with quick access to the aspect they need.

Statement numbering
A numbering system to allow easy reference for particular security controls.

Section heading
Indicates the particular topic covered within the section.

Explanatory text
Provides additional information about a particular term used in a statement.

Statement of Good Practice
Individually numbered statements that define the security controls to be applied in order to protect information and systems.

Section number and topic name
Provides quick access to the required section of the Standard.

Figure 5: Layout of each section within the Standard

The Principles and Objectives

The Principles and Objectives part of the Standard provides a high-level version of the Standard, by bringing together just the principles (which provide an overview of what needs to be performed to meet the Standard) and objectives (which outline the reason why these actions are necessary) for each section and presents them as shown in ***Figure 6***.

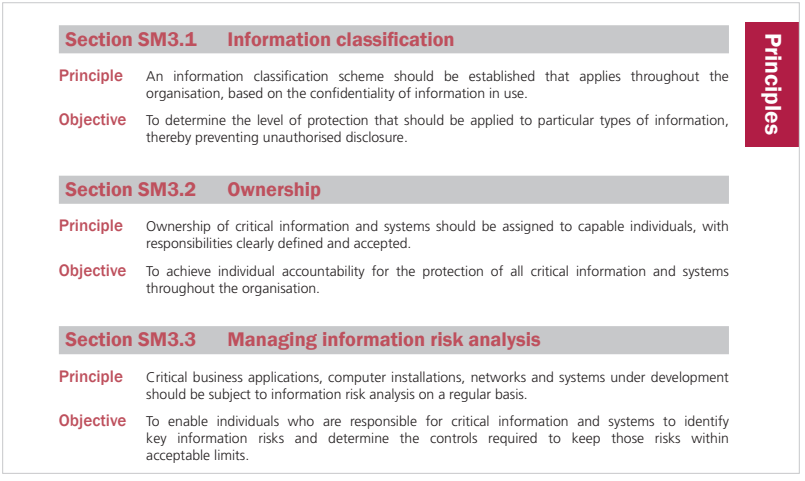
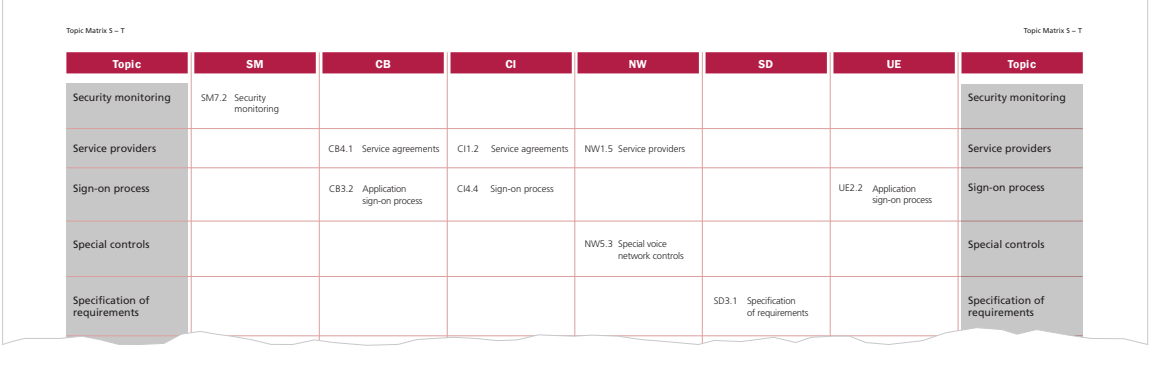


Figure 6: Principles and Objectives

The Topics Matrix

The Topics Matrix is a reference table that groups individual sections of the Standard under similar topic headings in alphabetical order (as shown in ***Figure 7***). It provides the reader with a quick and easy way of looking up particular topics in the Standard, irrespective of the Aspect in which they are located.



Topic	SM	CB	CI	NW	SD	UE	Topic
Security monitoring	SM7.2 Security monitoring						Security monitoring
Service providers		CB4.1 Service agreements	CI1.2 Service agreements	NW1.5 Service providers			Service providers
Sign-on process		CB3.2 Application sign-on process	CI4.4 Sign-on process			UE2.2 Application sign-on process	Sign-on process
Special controls				NW5.3 Special voice network controls			Special controls
Specification of requirements					SD3.1 Specification of requirements		Specification of requirements

Figure 7: Topics Matrix

Intro

The Index

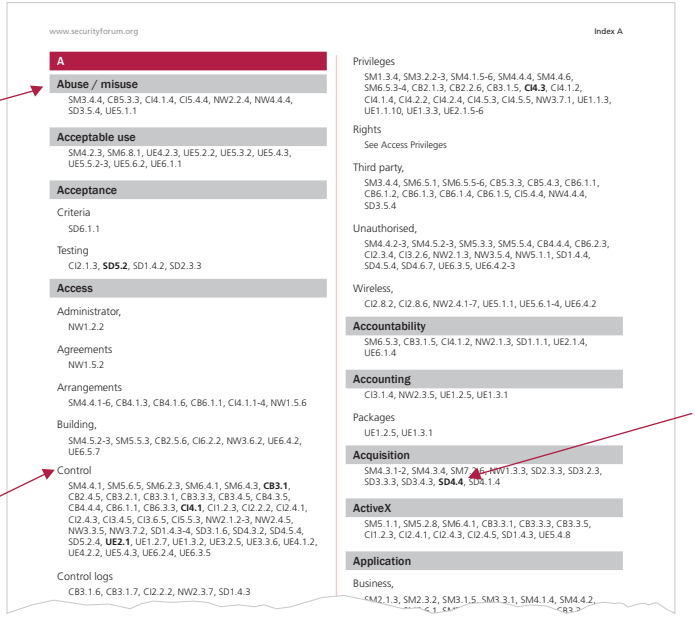
The Index presents an extensive alphabetical list of information security-related terms, concepts and topics, and provides a reference to the sections in which they are mentioned in the Standard (as shown in ***Figure 8***).

Main heading

Presents the key information security-related term, concept or topic used in the Standard. The corresponding reference(s) indicate each statement of good practice in the Standard where the term can be found.

Subheading

Indicates a prefix, suffix or associated term that relates to the main heading.



www.securityforum.org Index A

A

Abuse / misuse
SM3.4.4, CB5.3.3, CI4.1.4, CI5.4.4, NW2.2.4, NW4.4.4, SD3.5.4, UE5.1.1

Acceptable use
SM4.2.3, SM6.8.1, UE4.2.3, UE5.2.2, UE5.3.2, UE5.4.3, UE5.5.2-3, UE5.6.2, UE6.1.1

Acceptance
Criteria
SD6.1.1
Testing
CI2.1.3, **SD5.2**, SD1.4.2, SD2.3.3

Access
Administrator,
NW1.2.2
Agreements
NW1.5.2
Arrangements
SM4.4.1-6, CB4.1.3, CB4.1.6, CB6.1.1, CI4.1.1-4, NW1.5.6
Building,
SM4.5.2-3, SM5.5.3, CB2.5.6, CI6.2.2, NW3.6.2, UE6.4.2, UE6.5.7
Control
SM4.4.1, SM5.6.5, SM6.2.3, SM6.4.1, SM6.4.3, **CB3.1**, CB2.4.5, CB3.2.1, CB3.3.1, CB3.3.3, CB3.4.5, CB4.3.5, CB4.4.4, CB6.1.1, CB6.3.3, **CI4.1**, CI1.2.3, CI2.2.2, CI2.4.1, CI2.4.3, CI3.4.5, CI3.6.5, CI5.5.3, NW2.1.2-3, NW2.4.5, NW3.3.5, NW3.7.2, SD1.4.3-4, SD3.1.6, SD4.3.2, SD4.5.4, SD5.2.4, **UE2.1**, UE1.2.7, UE1.3.2, UE3.2.5, UE3.3.6, UE4.1.2, UE4.2.2, UE5.4.3, UE6.2.4, UE6.3.5
Control logs
CB3.1.6, CB3.1.7, CI2.2.2, NW2.3.7, SD1.4.3
Privileges
SM1.3.4, SM3.2.2-3, SM4.1.5-6, SM4.4.4, SM4.4.6, SM6.5.3-4, CB2.1.3, CB2.2.6, CB3.1.5, **CI4.3**, CI4.1.2, CI4.1.4, CI4.2.2, CI4.2.4, CI4.5.3, CI4.5.5, NW3.7.1, UE1.1.3, UE1.1.10, UE1.3.3, UE2.1.5-6
Rights
See Access Privileges
Third party,
SM3.4.4, SM6.5.1, SM6.5.5-6, CB5.3.3, CB5.4.3, CB6.1.1, CB6.1.2, CB6.1.3, CB6.1.4, CB6.1.5, CI5.4.4, NW4.4.4, SD3.5.4
Unauthorised,
SM4.4.2-3, SM4.5.2-3, SM5.3.3, SM5.5.4, CB4.4.4, CB6.2.3, CI2.3.4, CI3.2.6, NW2.1.3, NW3.5.4, NW5.1.1, SD1.4.4, SD4.5.4, SD4.6.7, UE6.3.5, UE6.4.2-3
Wireless,
CI2.8.2, CI2.8.6, NW2.4.1-7, UE5.1.1, UE5.6.1-4, UE6.4.2

Accountability
SM6.5.3, CB3.1.5, CI4.1.2, NW2.1.3, SD1.1.1, UE2.1.4, UE6.1.4

Accounting
CI3.1.4, NW2.3.5, UE1.2.5, UE1.3.1
Packages
UE1.2.5, UE1.3.1

Acquisition
SM4.3.1-2, SM4.3.4, SM7.2.6, NW1.3.3, SD2.3.3, SD3.2.3, SD3.3.3, SD3.4.3, **SD4.4**, SD4.1.4

ActiveX
SM5.1.1, SM5.2.8, SM6.4.1, CB3.3.1, CB3.3.3, CB3.3.5, CI1.2.3, CI2.4.1, CI2.4.3, CI2.4.5, SD1.4.3, UE5.4.8

Application
Business,
SM2.1.3, SM2.3.2, SM3.1.5, SM3.3.1, SM4.1.4, SM4.4.2,

Section reference

Where a heading or subheading relates to an entire section in the Standard, the reference is shown in bold.

Figure 8: Index

Benefits of using the Standard

Due to the versatility and comprehensive nature of the Standard, organisations can use it in many different ways, regardless of how they establish their own information security policies, standards and procedures.

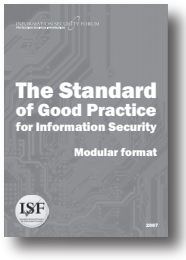
Whether it is used independently or in conjunction with ISF tools and other major information security-related standards, ***The Standard of Good Practice*** represents an unparalleled source of reference for information security.

The approach taken in developing ***The Standard of Good Practice*** ensures the content is comprehensive in its coverage of information security topics, is unambiguous and measurable. As a result, organisations can use the Standard to:

- ✓ Improve their information security policies, standards and procedures
- ✓ Measure the effectiveness of information security across the organisation*****
- ✓ Raise awareness of information security enterprise-wide
- ✓ Develop or improve information security controls
- ✓ Comply with internal and external information security requirements
- ✓ Undertake information risk analysis of important applications and systems.

*****ISF Members can use the ISF's ***Information Security Status Survey*** (the Survey) to measure their performance against ***The Standard of Good Practice***. The Survey is a practical, comprehensive, and automated benchmarking tool, which maps directly to the Standard. Using the Survey also allows Members to compare their performance with other leading organisations. Further details of how the Survey can be used with the Standard can be found in the report ***Making the most of the Standard***.

Additional information about ***The Standard of Good Practice*** can be found in the accompanying report entitled ***Making the most of the Standard***, which is available from the ISF's Member-only extranet (MX²), and also from the ISF's public website ***www.securityforum.org***.



The Standard of Good Practice is also available in a concise and modular format. This is also available from the ISF's Member-only extranet (MX²), and also from the ISF's public website ***www.securityforum.org***.

Principles and Objectives

Principles and Objectives

Overview of Principles and Objectives

Definition of principles and objectives 14
Breakdown of the Standard 14

Security Management (Enterprise-wide)

SM1 High-level direction 15
SM2 Security organisation 16
SM3 Security requirements 17
SM4 Secure environment 18
SM5 Malicious attack 20
SM6 Special topics 22
SM7 Management review 24

Critical Business Applications

CB1 Business requirements for security 25
CB2 Application management 26
CB3 User environment 28
CB4 System management 29
CB5 Local security management 30
CB6 Special topics 31

Computer Installations

CI1 Installation management 32
CI2 Live environment 33
CI3 System operation 35
CI4 Access control 37
CI5 Local security management 38
CI6 Service continuity 40

Networks

NW1 Network management 41
NW2 Traffic management 43
NW3 Network operations 44
NW4 Local security management 46
NW5 Voice networks 47

Systems Development

SD1 Development management 48
SD2 Local security management 49
SD3 Business requirements 50
SD4 Design and build 51
SD5 Testing 53
SD6 Implementation 54

End User Environment

UE1 Local security management 55
UE2 Corporate business applications 57
UE3 Desktop applications 58
UE4 Computing devices 59
UE5 Electronic communications 60
UE6 Environment management 62

Overview of Principles and Objectives

Definition of principles and objectives

Each section within *The Standard of Good Practice* includes a high-level principle and objective.

Each principle provides an overview of what needs to be done to meet the Standard and the objective outlines the reason why these actions are necessary.

Breakdown of the Standard

The Standard consists of six different aspects, each of which is broken down into summary areas and detailed sections. *Table 2* below shows the number of areas and sections found in each aspect.

Table 2: Breakdown of the Standard

Aspects	Number of areas	Number of sections
Security Management	7	36
Critical Business Applications	6	25
Computer Installations	6	31
Networks	5	25
Systems Development	6	23
End User Environment	6	26
Total	**36**	**166**

The full Standard is comprehensive, covers a large number of sections and is extremely detailed. However, a number of ISF Members have indicated that on some occasions they would prefer to review a high-level version of the Standard.

Consequently, this part of the Standard brings together just the principles and objectives for each section and presents them on the following pages.

Security Management

Keeping the business risks associated with information systems under control within an organisation requires clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the organisation and the establishment of a secure environment.

Area SM1
HIGH-LEVEL DIRECTION

Achieving an effective and consistent standard of good practice for information security throughout the organisation requires clear direction from the top. Accordingly, this area covers top management's direction on, and commitment to, information security. It specifies an information security policy and a set of staff agreements that should be applied to all individuals who have access to the information and systems of the organisation.

Section SM1.1 Management commitment

Principle Top management's direction on information security should be established, and commitment demonstrated.

Objective To ensure an appropriate set of security controls is implemented enterprise-wide.

Section SM1.2 Information security policy

Principle A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the organisation's information and systems.

Objective To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

Section SM1.3 Staff agreements

Principle Staff agreements should be established that specify information security responsibilities, are incorporated into staff contracts, and are taken into account when screening applicants for employment.

Objective To ensure that staff behave in a manner that supports the organisation's information security policy.

Area SM2
SECURITY ORGANISATION

Safeguarding information and systems requires information security activity to be organised effectively throughout the organisation. Accordingly, this area covers the organisational arrangements for managing information security throughout the organisation, raising security awareness amongst staff and ensuring they have the skills required to run systems correctly and securely.

Section SM2.1 High-level control

Principle Control over information security should be provided by a high-level working group, committee or equivalent body, and be supported by a top-level executive.

Objective To provide a top-down management structure and a practical mechanism for co-ordinating information security activity throughout the organisation.

Section SM2.2 Information security function

Principle A specialist information security function should be established, which has responsibility for promoting information security enterprise-wide.

Objective To ensure good practice in information security is applied effectively and consistently throughout the organisation.

Section SM2.3 Local security co-ordination

Principle Arrangements should be made to co-ordinate information security activity in individual business units / departments.

Objective To ensure that security activities are carried out in a timely and accurate manner, enterprise-wide, and that security issues are resolved effectively.

Section SM2.4 Security awareness

Principle Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the organisation.

Objective To ensure all relevant individuals apply security controls and prevent important information used throughout the organisation from being compromised or disclosed to unauthorised individuals.

Section SM2.5 Security education / training

Principle Staff should be educated / trained in how to run systems correctly and how to develop and apply information security controls.

Objective To provide staff with the skills required to protect systems and fulfil their information security responsibilities.

Area SM3
SECURITY REQUIREMENTS

Ensuring that the safeguards applied to information and systems are proportionate to their importance to the business is a fundamental element of good practice. Accordingly, this area covers arrangements for classifying critical information and systems, assigning ownership, managing information risk analysis, undertaking information risk analysis and legal and regulatory compliance.

Section SM3.1 Information classification

Principle An information classification scheme should be established that applies throughout the organisation, based on the confidentiality of information in use.

Objective To determine the level of protection that should be applied to particular types of information, thereby preventing unauthorised disclosure.

Section SM3.2 Ownership

Principle Ownership of critical information and systems should be assigned to capable individuals, with responsibilities clearly defined and accepted.

Objective To achieve individual accountability for the protection of all critical information and systems throughout the organisation.

Section SM3.3 Managing information risk analysis

Principle Critical business applications, computer installations, networks and systems under development should be subject to information risk analysis on a regular basis.

Objective To enable individuals who are responsible for critical information and systems to identify key information risks and determine the controls required to keep those risks within acceptable limits.

Section SM3.4 Information risk analysis methodologies

Principle Information risk analysis conducted on applications, computer installations, networks and systems under development should be undertaken using structured methodologies.

Objective To ensure information risk analysis is conducted in a consistent, rigorous and reliable manner throughout the organisation.

Section SM3.5 Legal and regulatory compliance

Principle A process should be established to identify and interpret the information security implications of relevant laws and regulations.

Objective To comply with laws and regulations affecting information security.

Area SM4
SECURE ENVIRONMENT

Achieving a consistent standard of good practice in information security across an organisation is a complex undertaking. The difficulties can be eased by introducing a common framework of disciplines and by making standard arrangements at organisation level, rather than on an individual basis (eg by developing a security architecture, establishing identity and access arrangements, creating a capability for managing information security incidents, and planning business continuity for the whole organisation). Accordingly, this area covers the arrangements required to build a secure environment enterprise-wide.

Section SM4.1 Security architecture

Principle A security architecture should be established, which provides a framework for the application of standard security controls throughout the organisation.

Objective To enable system developers and administrators to implement consistent, simple-to-use security functionality across multiple computer systems throughout the organisation.

Section SM4.2 Information privacy

Principle Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.

Objective To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.

Section SM4.3 Asset management

Principle Proven, reliable and approved hardware / software should be used that meet security requirements and are recorded in an inventory.

Objective To reduce the risk of information security being compromised by weaknesses in hardware / software.

Section SM4.4 Identity and access management

Principle Identity and access management arrangements should be established to provide effective and consistent user administration, identification, authentication and access mechanisms across the organisation.

Objective To restrict system access to authorised users and ensure the integrity of important user information.

Section SM4.5 Physical protection

Principle All locations that house critical IT facilities, sensitive material and other important assets should be physically protected against accident or attack.

Objective To restrict physical access to authorised individuals and ensure that critical IT facilities processing important information, sensitive material and other important assets are available when required.

(continued on the next page)

Section SM4.6 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

Section SM4.7 Business continuity

Principle Documented standards / procedures should be established for developing business continuity plans and for maintaining business continuity arrangements enterprise-wide.

Objective To enable the organisation to withstand the prolonged unavailability of critical information and systems.

Area SM5
MALICIOUS ATTACK

Organisations are often subject to attack from malicious third parties (eg by sending malware or hacking systems). Consequently, this area covers the security controls required to protect against malware, keep applications and systems up-to-date with patches, provide intrusion detection capabilities, respond to a serious attack and manage forensic investigations.

Section SM5.1 General malware protection

Principle All individuals who have access to information and systems of the organisation should be made aware of the risks from malware, and the actions required to minimise those risks.

Objective To ensure all relevant individuals understand the key elements of malware protection, why it is needed, and help to keep the impact of malware to a minimum.

Section SM5.2 Malware protection software

Principle Effective malware protection software should be installed, configured, and maintained enterprise-wide.

Objective To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales.

Section SM5.3 Intrusion detection

Principle Intrusion detection mechanisms should be applied to critical systems and networks.

Objective To identify suspected or actual malicious attacks and enable the organisation to respond before serious damage is done.

Section SM5.4 Emergency response

Principle An emergency response process should be established, supported by an emergency response team, which outlines actions to be taken in the event of a serious attack.

Objective To respond to serious attacks quickly and effectively, reducing any potential business impact.

Section SM5.5 Forensic investigations

Principle A process should be established for dealing with information security incidents that require forensic investigation.

Objective To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

(continued on the next page)

Section SM5.6 Patch management

Principle A process should be established for the deployment of system and software patches.

Objective To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

Area SM6
SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns that should be dealt with enterprise-wide. Accordingly, this area covers the special security controls that apply to the use of cryptography, public key infrastructure, electronic messaging, remote working, the provision of third party access, electronic commerce and outsourcing.

Section SM6.1 Cryptographic solutions

Principle Cryptographic solutions should be approved, documented and applied enterprise-wide.

Objective To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of information.

Section SM6.2 Public key infrastructure

Principle Where a public key infrastructure (PKI) is used, it should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.

Objective To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

Section SM6.3 E-mail

Principle E-mail systems should be protected by a combination of policy, awareness, procedural and technical security controls.

Objective To ensure that e-mail services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

Section SM6.4 Remote working

Principle Personal computers used by staff working in remote locations should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical and logical controls.

Objective To ensure that computers used by staff working in remote locations operate as intended, remain available and do not compromise the security of any facilities to which they can be connected.

Section SM6.5 Third party access

Principle Connections from third parties (eg customers, clients and suppliers) should be uniquely identified, subjected to an information risk analysis, approved, and supported by contracts.

Objective To ensure that access to the organisation's information and systems is restricted to authorised third parties.

(continued on the next page)

Section SM6.6 Electronic commerce

Principle A process should be established to ensure that information security requirements are taken into account in electronic commerce initiatives across the organisation.

Objective To keep the increased risks associated with the development and deployment of electronic commerce within acceptable limits.

Section SM6.7 Outsourcing

Principle A process should be established to govern the selection and management of outsource providers, supported by documented agreements that specify the security requirements to be met.

Objective To ensure that security requirements are satisfied and maintained when the running of a particular environment or service is entrusted to an outsource provider.

Section SM6.8 Instant messaging

Principle Instant messaging services should be protected by setting management policy, deploying instant messaging application controls and correctly configuring the security elements of an instant messaging infrastructure.

Objective To ensure that instant messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

Area SM7
MANAGEMENT REVIEW

An accurate understanding of the information security condition of the organisation is required in order to manage information security effectively. Accordingly, this area covers the arrangements needed to provide decision-makers with sound information on the security condition of information and systems throughout the organisation.

Section SM7.1 Security audit / review

Principle The information security status of critical IT environments should be subject to thorough, independent and regular security audits / reviews.

Objective To provide individuals who are responsible for particular IT environments, and top management, with an independent assessment of the information security condition of those environments.

Section SM7.2 Security monitoring

Principle The information security condition of the organisation should be monitored regularly and reported to top management.

Objective To provide top management with an accurate, comprehensive and coherent assessment of the security condition of the organisation.

Critical Business Applications

A critical business application requires a more stringent set of security controls than other applications. By understanding the business impact of a loss of confidentiality, integrity or availability of information, it is possible to establish the level of importance of an application. This provides a sound basis for identifying information risks and determining the level of protection required to keep information risks within acceptable limits.

Area CB1
BUSINESS REQUIREMENTS FOR SECURITY

Business applications vary enormously in their importance to the business; hence the level of protection required also varies. Accordingly, this area identifies the information security requirements of the application.

Section CB1.1 Confidentiality requirements

Principle The business impact of unauthorised disclosure of information associated with the application should be assessed.

Objective To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the application.

Section CB1.2 Integrity requirements

Principle The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the application should be assessed.

Objective To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the application.

Section CB1.3 Availability requirements

Principle The business impact of business information stored in or processed by the application being unavailable for any length of time should be assessed.

Objective To document and agree the availability requirements (the need for information to be accessible when required) of the application.

Area CB2
APPLICATION MANAGEMENT

Keeping business risks within acceptable limits requires a coherent set of information security arrangements. Accordingly, this area covers the roles and responsibilities required (including business ownership), integral application controls and additional controls needed for handling or transferring sensitive information. In addition, this area covers general management controls including change management, information security incident management and business continuity.

Principles

Section CB2.1 Roles and responsibilities

Principle An owner should be identified for the application, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To assign ownership of the application, achieve individual accountability, provide a sound management structure for staff running or using it and give responsible individuals a vested interest in its protection.

Section CB2.2 Application controls

Principle The full range of application controls should be considered, and required controls identified.

Objective To build in the required application controls to protect information stored in or processed by the application.

Section CB2.3 Change management

Principle Changes to the application should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise the security of the application.

Section CB2.4 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

Section CB2.5 Business continuity

Principle A business continuity plan should be established, supported by contingency arrangements, and tested regularly.

Objective To enable the business processes associated with the application to continue in the event of a disaster.

(continued on the next page)

Section CB2.6 Sensitive information

Principle Additional protection should be provided for applications that involve handling sensitive material or transferring sensitive information.

Objective To preserve the integrity of sensitive information and protect it from unauthorised disclosure.

Area CB3
USER ENVIRONMENT

Critical business applications can be used by internal or external business or technical users. These individuals may be sited locally or at a remote location, often with differing business and security requirements. Accordingly, this area covers the disciplines required to control access to the application, configure workstations and ensure that users are aware of information security and understand their personal responsibilities.

Section CB3.1 Access control

Principle Access to the application and associated information should be restricted to authorised individuals.

Objective To ensure that only authorised individuals are granted access to the application, and that individual accountability is assured.

Section CB3.2 Application sign-on process

Principle Users should be subject to a rigorous sign-on process before being provided with access to the application.

Objective To ensure that only authorised users can gain access to the application.

Section CB3.3 Workstation protection

Principle Workstations connected to the application should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements, and protected by physical controls.

Objective To ensure workstations operate as intended, are available when required and do not compromise the security of the application.

Section CB3.4 Security awareness

Principle Users of the application should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure users of the application apply security controls and prevent important information used in the application from being compromised or disclosed to unauthorised individuals.

Area CB4
SYSTEM MANAGEMENT

To enable applications to function, they have to run on one or more computers and typically make use of one or more networks. Accordingly, this area covers service agreements, the resilience of the application, external connections and the back-up of essential information and software.

Section CB4.1 Service agreements

Principle Computer and network services required to support the application should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.

Objective To define the business requirements for providers of any computer or network services that support the application, including those for information security, and to ensure they are met.

Section CB4.2 Resilience

Principle The application should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective To ensure that the application is available when required.

Section CB4.3 External connections

Principle All external connections to the application should be individually identified, verified, recorded, and approved.

Objective To ensure that only authorised individuals are granted access to the application via external connections.

Section CB4.4 Back-up

Principle Back-ups of essential information and software used by the application should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential information or software required by the application can be restored within critical timescales.

Area CB5
LOCAL SECURITY MANAGEMENT

The security controls applied to a business application should be proportional to business risk. Accordingly, this area covers the arrangements made to identify the importance of information stored in or processed by the application, the associated business risks and the level of protection required. It also addresses local security co-ordination and the need for the application to be subject to thorough, independent and regular security audits / reviews.

Section CB5.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate information security activities associated with the application.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

Section CB5.2 Information classification

Principle Information stored in or processed by critical business applications should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to the application, thereby preventing unauthorised disclosure.

Section CB5.3 Information risk analysis

Principle The application should be subject to an information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed.

Objective To identify key information risks associated with the application, and determine the security controls required in order to keep those risks within acceptable limits.

Section CB5.4 Security audit / review

Principle The information security status of the application should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls have been implemented effectively, that information risk is being managed, and to provide the application owner and top management with an independent assessment of the information security status of the application.

Area CB6
SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns. Where these topics apply to a critical business application, special security arrangements are required. Accordingly, this area covers the additional security controls required by applications that provide third party access, employ cryptographic key management, use a public key infrastructure (PKI) or are based on web-enabled technology.

Section CB6.1 Third party agreements

Principle Connections from third parties (ie external organisations, such as customers, suppliers and members of the public) should be subject to an information risk analysis, approved by the application owner and agreed by both parties in a documented agreement, such as a contract.

Objective To ensure that only approved third parties are granted access to the application.

Section CB6.2 Cryptographic key management

Principle Cryptographic keys should be managed tightly, in accordance with documented standards / procedures, and protected against unauthorised access or destruction.

Objective To ensure that cryptographic keys are not compromised (eg through loss, corruption or disclosure).

Section CB6.3 Public key infrastructure

Principle Any public key infrastructure (PKI) used by the application should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.

Objective To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

Section CB6.4 Web-enabled applications

Principle Specialised procedural and technical controls should be applied to web-enabled applications and the servers on which they run.

Objective To ensure that the increased risks associated with web-enabled applications are minimised.

Computer Installations

Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any computer installation (irrespective of where, or on what scale or types of computer it takes) a common standard of good practice for information security should be applied.

Area CI1
INSTALLATION MANAGEMENT

Computer installations used for processing information need to be well managed. Accordingly, this area covers the roles and responsibilities of the staff involved in running computer installations, agreements made with business users, management of key assets (eg hardware and software) and monitoring of the systems associated with the installation.

Section CI1.1 Roles and responsibilities

Principle An owner should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To achieve individual accountability for the computer installation, provide a sound management structure for staff running the installation and give responsible individuals a vested interest in its protection.

Section CI1.2 Service agreements

Principle Users' service requirements should be classified in a way that identifies their criticality to the business, and documented in contracts or service level agreements.

Objective To define the business requirements, including information security requirements, for services provided by the computer installation.

Section CI1.3 Asset management

Principle Essential information about hardware and software (eg unique identifiers, version numbers and physical locations) should be recorded in inventories, and software licensing requirements met.

Objective To protect information stored in or processed by the computer installation and to meet legal / regulatory requirements.

Section CI1.4 System monitoring

Principle Systems associated with the computer installation should be monitored continuously, and reviewed from a business user's perspective.

Objective To assess the performance of the computer installation, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

Area CI2
LIVE ENVIRONMENT

Service targets are more likely to be achieved if computer installations are designed well. Accordingly, this area covers the design of the installation, logging of key security-related events and the configuration of host systems and workstations. It also covers the resilience of the installation and its protection from physical loss or damage.

Section CI2. 1 Installation design

Principle Computer installations should be designed to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.

Objective To produce a computer installation that has security functionality built-in and enables additional controls to be incorporated easily.

Section CI2.2 Security event logging

Principle Important security-related events should be recorded in logs, stored centrally, protected against unauthorised change and analysed on a regular basis.

Objective To identify threats that may lead to an information security incident, and maintain the integrity of important security-related information.

Section CI2.3 Host system configuration

Principle Host systems should be configured to function as required, and to prevent unauthorised or incorrect updates.

Objective To ensure host systems operate as intended and do not compromise the security of the computer installation.

Section CI2.4 Workstation protection

Principle Workstations connected to systems within the computer installation should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements, and protected by physical and logical controls.

Objective To ensure workstations operate as intended and do not compromise the security of the systems to which they are connected.

Section CI2.5 Resilience

Principle The computer installation should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective To ensure that the systems supported by the computer installation are available when required.

(continued on the next page)

Section CI2.6 Hazard protection

Principle Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.

Objective To prevent services being disrupted by damage to computer equipment or facilities caused by fire, flood and other types of hazard.

Section CI2.7 Power supplies

Principle Critical computer equipment and facilities should be protected against power outages.

Objective To prevent services provided by the computer installation from being disrupted by loss of power.

Section CI2.8 Physical access

Principle Physical access to critical computer installation facilities should be restricted to authorised individuals.

Objective To prevent services being disrupted by loss of or damage to equipment or facilities.

Area CI3
SYSTEM OPERATION

Achieving service targets requires computer installations to be run in accordance with sound disciplines. Accordingly, this area covers basic controls over system operation (ie handling computer media, back-up and change management) and arrangements for identifying and resolving incidents (ie information security incident management and emergency fixes).

Section CI3.1 Handling computer media

Principle Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure, and additional security controls applied to media containing sensitive information.

Objective To protect computer media in accordance with information security and regulatory requirements.

Section CI3.2 Back-up

Principle Back-ups of essential information and software used by the computer installation should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential information and software required by the installation can be restored within critical timescales.

Section CI3.3 Change management

Principle Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise the security of the installation.

Section CI3.4 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

Section CI3.5 Emergency fixes

Principle Emergency fixes to computer equipment, business applications, systems software and business information should be tested, reviewed and applied quickly and effectively, in accordance with documented standards / procedures.

Objective To respond to emergencies in a timely and secure manner, while reducing disruption to the organisation.

(continued on the next page)

Section CI3.6 Patch management

Principle A process should be established for managing the application of system and software patches, which is supported by documented standards / procedures.

Objective To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

Area CI4
ACCESS CONTROL

Effective access control mechanisms can reduce the risk of unauthorised access to information and systems. Accordingly, this area covers the access control disciplines applied to users and the steps taken to restrict access to information and systems within the computer installation.

Section CI4.1 Access control arrangements

Principle Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation.

Objective To ensure that only authorised individuals gain access to information or systems within the computer installation, and that individual accountability is assured.

Section CI4.2 User authorisation

Principle All users of the computer installation should be authorised before they are granted access privileges.

Objective To restrict access to any information or systems within the computer installation to authorised users.

Section CI4.3 Access privileges

Principle All users of the computer installation should be assigned specific privileges to allow them to access particular information or systems.

Objective To provide authorised users with access privileges which are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

Section CI4.4 Sign-on process

Principle Users should follow a rigorous system sign-on process before being provided with access to target systems.

Objective To prevent unauthorised users from gaining access to any information or systems within the computer installation.

Section CI4.5 User authentication

Principle All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (eg smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.

Objective To prevent unauthorised users from gaining access to any information or systems within the computer installation.

Area CI5
LOCAL SECURITY MANAGEMENT

A computer installation typically supports one or more critical business applications, holds information that needs to be protected, and is an important asset in its own right. Each of these perspectives needs to be considered in order to provide appropriate protection. Accordingly, this area covers the arrangements made to identify the relative importance of the computer installation, the associated business risks and the level of protection required. It also covers the arrangements made to ensure that information security is co-ordinated locally, staff are aware of information security and understand their personal responsibilities, and the need for the installation to be subject to thorough, independent and regular security audits / reviews.

Section CI5.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate the information security activities associated with the computer installation.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

Section CI5.2 Security awareness

Principle Individuals running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure individuals running the installation apply security controls and prevent important information stored in or processed by the installation from being compromised or disclosed to unauthorised individuals.

Section CI5.3 Information classification

Principle Information stored or processed within the computer installation should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to the computer installation, thereby preventing unauthorised disclosure.

Section CI5.4 Information risk analysis

Principle The computer installation should be subject to an information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed.

Objective To identify key information risks associated with the computer installation and determine the security controls required in order to keep those risks within acceptable limits.

(continued on the next page)

Section CI5.5 Security audit / review

Principle The information security status of the computer installation should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls have been implemented effectively, that risk is being managed and to provide the installation owner, and top management, with an independent assessment of the security status of the installation.

Area CI6
SERVICE CONTINUITY

If there is a serious interruption to information processing, (eg if a disaster occurs), the computer installation may be unavailable for a prolonged period. Considerable forethought is required to enable information processing to continue in these circumstances and to keep the business impact to a minimum. Accordingly, this area covers the development of contingency plans and arrangements, and their validation.

Section CI6.1 Contingency plans

Principle A contingency plan should be developed and documented.

Objective To provide individuals with a documented set of actions to perform in the event of a disaster, enabling information processing to be resumed within critical timescales.

Section CI6.2 Contingency arrangements

Principle Alternative processing arrangements should be established, and made available when required.

Objective To enable information processing to resume within critical timescales, using alternative facilities.

Section CI6.3 Validation and maintenance

Principle Contingency plans and arrangements should be tested on a regular basis.

Objective To ensure that information processing can resume within critical timescales, using alternative facilities.

Networks

Computer networks convey information and provide a channel of access to information systems. By their nature, they are highly vulnerable to disruption and abuse. Safeguarding business communications requires robust network design, well-defined network services, and sound disciplines to be observed in running networks and managing security. These factors apply equally to local and wide area networks, and to data and voice communications.

Area NW1
NETWORK MANAGEMENT

Computer networks are complex. They have to link different systems together, are subject to constant change and often rely on services provided by external parties. Orchestrating the technical and organisational issues involved requires sound management. Accordingly, this area covers the organisational arrangements for running a network, its design, resilience and documentation, and the management of relationships with service providers.

Section NW1.1 Roles and responsibilities

Principle An owner should be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To achieve individual accountability for the network, provide a sound management structure for staff running the network and give responsible individuals a vested interest in its protection.

Section NW1.2 Network design

Principle The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.

Objective To produce an operational network that has security functionality built-in and enables additional controls to be incorporated easily.

Section NW1.3 Network resilience

Principle The network should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective To ensure that the network is available when required.

Section NW1.4 Network documentation

Principle Networks should be supported by accurate, up-to-date documentation.

Objective To ensure that the network is configured accurately and securely.

(continued on the next page)

Section NW1.5 Service providers

Principle Network services should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.

Objective To define the business requirements for network service providers, including those for security, and ensure they are met.

Area NW2
TRAFFIC MANAGEMENT

Computer networks can handle many types of traffic from a wide variety of sources. To manage network traffic effectively, network devices (eg firewalls) have to be configured correctly and particular types of network traffic denied access. Accordingly, this area covers the disciplines required to ensure undesirable network traffic and unauthorised external or wireless users are prevented from gaining access to the network.

Section NW2.1 Configuring network devices

Principle Network devices (eg firewalls) should be configured to function as required, and to prevent unauthorised or incorrect updates.

Objective To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

Section NW2.2 Firewalls

Principle Network traffic should be routed through a well-configured firewall, prior to being allowed access to the network, or before leaving the network.

Objective To prevent unauthorised network traffic from gaining access to the network, or leaving the network.

Section NW2.3 External access

Principle All external connections to the network should be individually identified, verified, recorded, and approved by the network owner.

Objective To prevent unauthorised external users from gaining access to the network.

Section NW2.4 Wireless access

Principle Wireless access should be authorised, users authenticated, and wireless traffic encrypted.

Objective To ensure that only authorised individuals gain wireless access to the network and minimise the risk of wireless transmissions being monitored, intercepted or modified.

Area NW3
NETWORK OPERATIONS

Maintaining continuity of service to users requires computer networks to be run in accordance with sound disciplines. Accordingly, this area covers the arrangements needed to monitor network performance and to manage changes and information security incidents. In addition, the area covers the arrangements required to provide physical security, perform back-ups and ensure service continuity.

Section NW3.1 Network monitoring

Principle Network activity should be monitored using a range of techniques such as capacity planning; review of network and intrusion detection logs; and examination of usage reports from service providers.

Objective To assess the performance of the network, reduce the likelihood of network overload and detect potential or actual malicious intrusions.

Section NW3.2 Change management

Principle Changes to the network should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise the security of the network.

Section NW3.3 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve network information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

Section NW3.4 Physical security

Principle Physical access to critical network facilities should be restricted to authorised individuals.

Objective To prevent services being disrupted by loss of, or damage to, communications equipment, power or facilities.

Section NW3.5 Back-up

Principle Back-ups of essential information and software used by the network should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential network information or software required by the network can be restored within critical timescales.

(continued on the next page)

Section NW3.6 Service continuity

Principle A service continuity plan should be established, supported by effective contingency arrangements, and tested regularly.

Objective To enable critical network services to continue in the event of a disaster.

Section NW3.7 Remote maintenance

Principle Remote maintenance of the network should be restricted to authorised individuals, confined to individual sessions, and subject to review.

Objective To prevent unauthorised access to the network through the misuse of remote maintenance facilities.

Area NW4
LOCAL SECURITY MANAGEMENT

Computer networks play an essential role in the functioning of many critical business applications. They convey information that needs to be protected, and are valuable assets in their own right. Accordingly, this area covers the arrangements made to identify the relative importance of the network, the associated business risks and the level of protection required. The area also covers the arrangements made to ensure that information security is co-ordinated locally, network staff are aware of information security and understand their personal responsibilities, and the need for the network to be subject to thorough, independent and regular security audits / reviews.

Section NW4.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate the information security activities associated with the network.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

Section NW4.2 Security awareness

Principle Individuals maintaining the network should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure individuals maintaining the network apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.

Section NW4.3 Information classification

Principle Information transmitted over the network should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to the network, thereby preventing unauthorised disclosure.

Section NW4.4 Information risk analysis

Principle The network should be subject to an information risk analysis on a regular basis, the results of which should be documented, reviewed and agreed.

Objective To identify key information risks associated with the network and determine the security controls required in order to keep those risks within acceptable limits.

Section NW4.5 Security audit / review

Principle The information security status of the network should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls have been implemented effectively, that information risk is being managed and to provide the network owner, and top management, with an independent assessment of the security status of the network.

Area NW5
VOICE NETWORKS

Business processes can be disrupted if voice networks, such as telephone systems, are unavailable or overloaded. Harm can also be caused if voice networks are subject to unauthorised use by outsiders, or sensitive conversations are overheard. Accordingly, this area covers the security arrangements applied to traditional voice and Voice over IP (VoIP) networks.

Section NW5.1 Voice network documentation

Principle Voice networks should include documentation of essential components and be supported by documented standards / procedures.

Objective To provide employees with a clear statement of the security disciplines they are expected to follow in relation to voice networks.

Section NW5.2 Resilience of voice networks

Principle Voice networks should be supported by a robust and reliable set of hardware and software, and be supported by alternative facilities.

Objective To ensure that voice network facilities (eg telephone exchanges) are available when required.

Section NW5.3 Special voice network controls

Principle Voice network facilities (eg telephone exchanges) should be monitored regularly and access to them restricted.

Objective To prevent and detect unauthorised use or misuse of voice network facilities.

Section NW5.4 Voice over IP (VoIP) networks

Principle Voice over IP (VoIP) networks should be approved, and protected by a combination of general, network and VoIP-specific controls.

Objective To ensure the availability of the VoIP network, and protect the confidentiality and integrity of sensitive information (eg the content of telephone calls) in transit.

Systems Development

Building security into systems during their development is more cost-effective and secure than applying it afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.

Area SD1
DEVELOPMENT MANAGEMENT

Producing robust systems, on which the organisation can depend, requires a sound approach to systems development. Accordingly, this area covers the organisation of systems development staff, the methodology used in developing systems, quality assurance and the security of development environments.

Section SD1.1 Roles and responsibilities

Principle An individual should be appointed to manage systems development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To achieve individual accountability for systems development activities and provide a sound management structure for staff performing them.

Section SD1.2 Development methodology

Principle Development activities should be carried out in accordance with a documented system development methodology.

Objective To ensure that systems under development meet business requirements, including those for information security.

Section SD1.3 Quality assurance

Principle Quality assurance of key security activities should be performed during the system development life cycle.

Objective To provide assurance that security requirements are defined adequately, agreed security controls are developed, and security requirements are met.

Section SD1.4 Development environments

Principle System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.

Objective To provide a secure environment for system development activities, and avoid any disruption to mainstream business activity.

Area SD2
LOCAL SECURITY MANAGEMENT

In common with live systems, systems under development need to be supported by a sound organisational structure and run by individuals who are aware of information security and know how to apply security controls effectively. Accordingly, this area covers the arrangements made to ensure that information security is co-ordinated locally, systems development staff are aware of information security and understand their personal responsibilities, and the need for systems development activities to be subject to thorough, independent and regular security audits / reviews.

Section SD2.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate information security activities associated with systems development.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that information security issues are resolved effectively.

Section SD2.2 Security awareness

Principle Systems developers should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure systems developers apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.

Section SD2.3 Security audit / review

Principle The information security status of systems development activity should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls are designed effectively, that risk is managed, and to provide the business owner and top management, with an independent assessment of the information security status of systems development activities.

Area SD3
BUSINESS REQUIREMENTS

A thorough understanding of business requirements (including those for the confidentiality, integrity and availability of information) is essential if systems are to fulfil their intended purpose. Accordingly, this area covers the arrangements made for specifying business requirements, determining security requirements and conducting information risk analyses.

Section SD3.1 Specification of requirements

Principle Business requirements (including those for information security) should be documented and agreed before detailed design commences.

Objective To ensure that information security requirements are treated as an integral part of business requirements, fully considered and approved.

Section SD3.2 Confidentiality requirements

Principle The business impact of unauthorised disclosure of business information stored in or processed by the system under development should be assessed.

Objective To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the system under development.

Section SD3.3 Integrity requirements

Principle The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the system under development should be assessed.

Objective To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the system under development.

Section SD3.4 Availability requirements

Principle The business impact of business information stored in or processed by the system under development being unavailable for any length of time should be assessed.

Objective To document and agree the availability requirements (the need for information to be accessible when required) of the system under development.

Section SD3.5 Information risk analysis

Principle Systems under development should be subject to a structured information risk analysis, the results of which should be documented, reviewed and agreed.

Objective To identify key information risks associated with critical systems under development and determine the security controls required in order to keep those risks within acceptable limits.

Area SD4
DESIGN AND BUILD

Building systems that function as intended requires the use of sound disciplines throughout the design and build stage of development. Accordingly, this area covers the arrangements needed to address information security during design, acquisition and system build, and the identification of required application, general and web-specific security controls.

Section SD4.1 System design

Principle Information security requirements for the system under development should be considered when designing the system.

Objective To produce a live system based on sound design principles which has security functionality built-in and enables controls to be incorporated easily.

Section SD4.2 Application controls

Principle The full range of application controls should be considered when designing the system under development.

Objective To ensure that required application controls are built-in to the system under development.

Section SD4.3 General security controls

Principle The full range of general security controls should be considered when designing the system under development.

Objective To ensure that required general security controls are established to support the system under development.

Section SD4.4 Acquisition

Principle Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.

Objective To ensure that hardware and software acquired from third parties provides the required functionality and does not compromise the security of systems under development.

Section SD4.5 System build

Principle System build activities (including coding and package customisation) should be carried out in accordance with industry good practice; performed by individuals provided with adequate skills / tools; and inspected to identify unauthorised modifications or changes.

Objective To ensure that systems are built correctly, able to withstand malicious attacks, and that no security weaknesses are introduced during the build process.

(continued on the next page)

Section SD4.6 Web-enabled development

Principle Specialised technical security controls should be applied to the development of web-enabled applications.

Objective To ensure that the increased risks associated with the development of web-enabled applications are minimised.

Area SD5
TESTING

Testing is a fundamental element of good practice in systems development. Planned well and performed correctly, it provides assurance that systems, including security controls, function as intended and reduces the likelihood of system malfunctions occurring. Accordingly, this area covers the arrangements needed to carry out testing thoroughly, without disrupting other activities.

Section SD5.1 Testing process

Principle All elements of a system (including application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.

Objective To ensure systems function correctly and meet security requirements.

Section SD5.2 Acceptance testing

Principle Systems under development should be subject to rigorous acceptance testing in a separate area that simulates the live environment.

Objective To ensure that newly developed systems function as intended and do not compromise information security.

Area SD6
IMPLEMENTATION

Sound disciplines are required when new systems are promoted from the development into the live environment. Accordingly, this area covers system promotion criteria, the installation of new systems in the live environment and post-implementation reviews.

Section SD6.1 System promotion criteria

Principle Rigorous criteria should be met before new systems are promoted into the live environment.

Objective To ensure that only tested and approved versions of hardware and software are promoted into the live environment.

Section SD6.2 Installation process

Principle New systems should be installed in the live environment in accordance with a documented installation process.

Objective To minimise disruption to the organisation when new systems are installed in the live environment.

Section SD6.3 Post-implementation review

Principle Post-implementation reviews should be conducted for all new systems.

Objective To check that systems and information security controls function as intended.

End User Environment

Individuals in end user environments typically have access to corporate applications that are critical to the organisation and often develop critical desktop applications using powerful spreadsheets or databases. Furthermore, sensitive information can be processed or stored on local computing devices such as personal computers, hand-held devices or portable storage devices. Protecting this information is essential, and requires a combination of enterprise-driven and local activities, such as effective local security management; controlling access to corporate business applications; identifying and protecting important desktop applications; securing computing devices and electronic communications (eg e-mail, instant messaging and Internet access); and implementing effective business continuity arrangements.

Area UE1
LOCAL SECURITY MANAGEMENT

Minimising information risks within the end user environment requires effective security management and the contribution of all individuals. Accordingly, this area covers roles and responsibilities, user awareness, and training. It also addresses local security co-ordination and information classification.

Section UE1.1 Roles and responsibilities

Principle An owner should be identified for the end user environment, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To assign ownership of the end user environment, provide a sound management structure for staff and give responsible individuals a vested interest in the protection of the end user environment.

Section UE1.2 Security awareness

Principle Users should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure users apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.

Section UE1.3 User training

Principle Users should be trained in how to run systems correctly and how to develop and apply security controls.

Objective To provide users with the skills required to protect systems and fulfil their information security responsibilities.

(continued on the next page)

Section UE1.4 Local security co-ordination

Principle An individual should be appointed to co-ordinate information security activities in the end user environment.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

Section UE1.5 Information classification

Principle Information stored in or processed by applications and systems in the end user environment should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to applications and systems in the end user environment, thereby preventing unauthorised disclosure.

Area UE2 CORPORATE BUSINESS APPLICATIONS

Corporate business applications accessible from the end user environment should be protected from unauthorised access and the adverse consequences of change. Accordingly, this area covers the disciplines required to restrict access to corporate business applications and to ensure that changes made do not cause adverse business impact.

Section UE2.1 Access control

Principle Access to corporate systems should be restricted to authorised individuals.

Objective To ensure that only authorised individuals are granted access to corporate systems, and that individual accountability is assured.

Section UE2.2 Application sign-on process

Principle Users should be subject to a rigorous sign-on process before they are provided with access to corporate business applications.

Objective To ensure that only authorised users are granted access to corporate business applications.

Section UE2.3 Change management

Principle Changes to corporate business applications accessible from the end user environment should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise security.

Area UE3
DESKTOP APPLICATIONS

Protecting critical desktop applications in the end user environment, and the accuracy of the information they store or process, requires a combination of good practice in general information security, supported by a set of technical security controls specific to desktop applications. Accordingly, this area covers the recording of critical desktop applications in an inventory, the development of critical desktop applications, and their protection.

Section UE3.1 Inventory of desktop applications

Principle Critical desktop applications used in the end user environment should be recorded in an inventory, or equivalent.

Objective To maintain an accurate and up-to-date record of critical desktop applications in the end user environment, enabling them to be protected accordingly.

Section UE3.2 Protection of spreadsheets

Principle Critical desktop applications created using spreadsheet programs should be protected by validating input, implementing access control, and restricting access to powerful functionality.

Objective To assure the accuracy of information processed by critical spreadsheets, and protect that information from disclosure to unauthorised individuals.

Section UE3.3 Protection of databases

Principle Critical desktop applications created using database programs should be protected by validating input, implementing access control, and restricting access to powerful functionality.

Objective To assure the accuracy of information processed by critical databases, and protect that information from disclosure to unauthorised individuals.

Section UE3.4 Desktop application development

Principle Development of desktop applications should be carried out in accordance with a documented development methodology.

Objective To ensure desktop applications function correctly and meet security requirements.

Area UE4
COMPUTING DEVICES

The protection of computing devices used in the end user environment (and the information they store or process) requires a combination of both physical and logical controls to be applied. Accordingly, this area covers the disciplines required to configure, maintain and protect workstations, hand-held devices and portable storage devices.

Section UE4.1 Workstation protection

Principle Workstations used in the end user environment should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical and logical controls.

Objective To ensure workstations operate as intended, are available when required and do not compromise the security of information stored in or processed by them.

Section UE4.2 Hand-held devices

Principle Hand-held devices (eg Personal Digital Assistants (PDAs), WAP-based mobile phones and smartphones) used in the end user environment should be approved, protected by software controls and supported by standards / procedures for acceptable use.

Objective To ensure hand-held devices operate as intended, are available when required and do not compromise the security of information stored in or processed by them.

Section UE4.3 Portable storage devices

Principle The use of portable storage devices in the end user environment should be approved, access to them restricted, and information stored on them protected.

Objective To ensure that important information stored on portable storage devices is protected from unauthorised disclosure.

Area UE5
ELECTRONIC COMMUNICATIONS

Electronic communication in the end user environment should be subject to a range of controls which preserve the accuracy and confidentiality of information whilst also protecting the organisation from unintended consequences which may result from misuse of communications facilities. Accordingly, this area covers the approved use of electronic communications, end user behaviour when using electronic communication as well as the application of specific controls relating to e-mail; instant messaging; use of the Internet; Voice over IP (VoIP) networks; and wireless access.

Section UE5.1 General controls

Principle — The use of electronic communications (eg e-mail, instant messaging, Internet access, Voice over IP or wireless access) should be supported by setting policy covering the types of communication permitted, and promoting user awareness of the security issues associated with their use.

Objective — To ensure that the organisation's reputation is not damaged as a result of the transmission of inappropriate information, that the content of electronic communications is accurate, and that business activity is not disrupted by the introduction of malware.

Section UE5.2 E-mail

Principle — Use of e-mail systems should be approved, and protected by a combination of policy, awareness, and procedural controls.

Objective — To ensure that the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

Section UE5.3 Instant messaging

Principle — Use of instant messaging services should be approved, and protected by setting management policy, deploying instant messaging application controls and correctly configuring the security elements of an instant messaging infrastructure.

Objective — To ensure that instant messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

Section UE5.4 Internet access

Principle — Use of the Internet by end users should be approved, and protected by restricting the types of use permitted, deploying approved web browsers and promoting awareness of the risks associated with Internet access.

Objective — To ensure that use of the Internet is restricted to legitimate business activity and that the risks associated with malicious code are minimised.

(continued on the next page)

Section UE5.5 Voice over IP (VoIP) networks

Principle Voice over IP (VoIP) networks should be approved, and protected by a combination of general network and VoIP-specific controls.

Objective To ensure the availability of the VoIP network, protect the confidentiality and integrity of sensitive information in transit, and minimise the risk of misuse.

Section UE5.6 Wireless access

Principle Wireless access should be authorised, users authenticated and wireless traffic encrypted.

Objective To ensure that only authorised individuals can gain wireless access to the network, and minimise the risk of wireless transmissions being monitored, intercepted or modified.

Area UE6
ENVIRONMENT MANAGEMENT

End user environments are important to the success of the organisation, therefore security arrangements within the end user environment should reflect those made on an enterprise-wide basis. Accordingly, this area covers the protection of personally identifiable information; information security incident management; back-up of important information and software; physical protection of the end user environment; and business continuity.

Section UE6.1 Information privacy

Principle Approved methods for handling personally identifiable information should be established and applied.

Objective To prevent information about individuals being used in an inappropriate manner, and to ensure compliance with legal and regulatory requirements for information privacy.

Section UE6.2 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar information security incidents occurring.

Section UE6.3 Back-up

Principle Back-ups of essential information, applications and software used in the end user environment should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential information or software required in the end user environment can be restored within critical timescales.

Section UE6.4 Physical and environmental protection

Principle The end user environment (and sensitive material stored within it) should be subject to a range of physical and environmental controls.

Objective To restrict physical access to authorised individuals and ensure that IT facilities processing critical information are available when required.

Section UE6.5 Business continuity

Principle A business continuity plan should be established, supported by contingency arrangements, and tested regularly.

Objective To enable the business processes associated with the end user environment to continue in the event of a disaster.

Topics Matrix

Overview of Topics Matrix

The Standard of Good Practice provides a practical, business focused and achievable statement of 'good practice' for information security.

The Standard is structured to cover the full spectrum of security-related topics in the form of six different aspects: Security Management (enterprise-wide); Critical Business Applications; Computer Installations; Networks; Systems Development; and End User Environment.

The structure of the Standard provides organisations with a simple and effective way to obtain a detailed breakdown of information security-related topics for particular environments. Consequently, each aspect within the Standard has been designed to 'stand alone', and can be used independently for a particular type of environment (such as a critical business application).

However, such a structure means that there is some repetition of topics across aspects. Consequently, the ISF has created a topics matrix to group individual sections of the Standard under similar topic headings in alphabetical order. For example, sections that have been categorised under the topic of 'Sign-on process' include CB3.2 Application sign-on process, CI4.4 Sign-on process and UE2.2 Application sign-on process, as shown in ***Figure 9***.

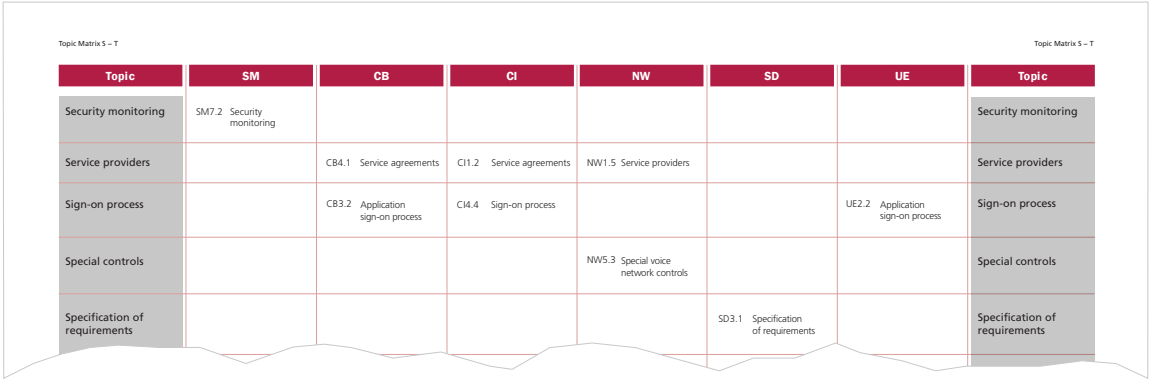


Figure 9: Layout of the Topics Matrix

The topics matrix is presented on the following pages.

Members can also use ***The Standard of Good Practice*** in modular format. This is an electronic version of the Standard that is organised to present the same set of security-related topics while avoiding the repetition, resulting in a concise set of control statements.

The Standard of Good Practice (in modular format) is aligned with the ISF's Security Healthcheck, enabling Members to perform a 'quick and easy' assessment of the status of security within a particular environment.

Topic	SM	CB	CI
Access control		CB3.1 Access control	CI4.1 Access control arrangements CI4.3 Access privileges
Acquisition			
Application controls		CB2.2 Application controls	
Asset management	SM4.3 Asset management		CI1.3 Asset management
Availability requirements		CB1.3 Availability requirements	
Back-up		CB4.4 Back-up	CI3.2 Back-up
Business continuity	SM4.7 Business continuity	CB2.5 Business continuity	CI6.1 Contingency plans CI6.2 Contingency arrangements CI6.3 Validation and maintenance
Change management		CB2.3 Change management	CI3.3 Change management
Confidentiality requirements		CB1.1 Confidentiality requirements	
Configuring network devices			
Cryptography	SM6.1 Cryptographic solutions	CB6.2 Cryptographic key management	
Development methodologies and environment			
E-mail	SM6.3 E-mail		
Electronic commerce	SM6.6 Electronic commerce		
Emergency fixes			CI3.5 Emergency fixes

NW	SD	UE	Topic
		UE2.1 Access control	Access control
	SD4.4 Acquisition		Acquisition
	SD4.2 Application controls	UE3.2 Protection of spreadsheets UE3.3 Protection of databases	Application controls
			Asset management
	SD3.4 Availability requirements		Availability requirements
NW3.5 Back-up		UE6.3 Back-up	Back-up
NW3.6 Service continuity		UE6.5 Business continuity	Business continuity
NW3.2 Change management		UE2.3 Change management	Change management
	SD3.2 Confidentiality requirements		Confidentiality requirements
NW2.1 Configuring network devices			Configuring network devices
			Cryptography
	SD1.2 Development methodology SD1.4 Development environments	UE3.4 Desktop application development	Development methodologies and environment
		UE5.2 E-mail	E-mail
			Electronic commerce
			Emergency fixes

Topic	SM	CB	CI
External access / connections		CB4.3 External connections	
Firewalls			
Forensic investigations	SM5.5 Forensic investigations		
General security controls			
Hand-held devices			
Handling information		CB2.6 Sensitive information	CI3.1 Handling computer media
Hazard protection			CI2.6 Hazard protection
Host system configuration			CI2.3 Host system configuration
Identity and access management	SM4.4 Identity and access management		
Information classification	SM3.1 Information classification	CB5.2 Information classification	CI5.3 Information classification
Information privacy	SM4.2 Information privacy		
Information risk analysis	SM3.3 Managing information risk analysis SM3.4 Information risk analysis methodologies	CB5.3 Information risk analysis	CI5.4 Information risk analysis
Information security function	SM2.2 Information security function		
Information security incident management	SM4.6 Information security incident management SM5.4 Emergency response	CB2.4 Information security incident management	CI3.4 Information security incident management
Information security policy	SM1.2 Information security policy		
Installation and network design			CI2.1 Installation design

NW	SD	UE	Topic
NW2.3 External access			External access / connections
NW2.2 Firewalls			Firewalls
			Forensic investigations
	SD4.3 General security controls	UE5.1 General controls	General security controls
		UE4.2 Hand-held devices	Hand-held devices
			Handling information
			Hazard protection
			Host system configuration
			Identity and access management
NW4.3 Information classification		UE1.5 Information classification	Information classification
		UE6.1 Information privacy	Information privacy
NW4.4 Information risk analysis			Information risk analysis
	SD3.5 Information risk analysis		Information security function
NW3.3 Information security incident management		UE6.2 Information security incident management	Information security incident management
			Information security policy
NW1.2 Network design			Installation and network design

Topic	SM	CB	CI
Installation process			
Instant messaging	SM6.8 Instant messaging		
Integrity requirements		CB1.2 Integrity requirements	
Internet access			
Intrusion detection	SM5.3 Intrusion detection		
Inventory of desktop applications			
Legal and regulatory compliance	SM3.5 Legal and regulatory compliance		
Local security co-ordination	SM2.3 Local security co-ordination	CB5.1 Local security co-ordination	CI5.1 Local security co-ordination
Malware protection	SM5.1 General malware protection SM5.2 Malware protection software		
Management commitment	SM1.1 Management commitment SM2.1 High-level control		
Network documentation			
Outsourcing	SM6.7 Outsourcing		
Patch management	SM5.6 Patch management		CI3.6 Patch management
Physical protection	SM4.5 Physical protection		CI2.8 Physical access

NW	SD	UE	Topic
	SD6.2 Installation process		Installation process
		UE5.3 Instant messaging	Instant messaging
	SD3.3 Integrity requirements		Integrity requirements
		UE5.4 Internet access	Internet access
			Intrusion detection
		UE3.1 Inventory of desktop applications	Inventory of desktop applications
			Legal and regulatory compliance
NW4.1 Local security co-ordination	SD2.1 Local security co-ordination	UE1.4 Local security co-ordination	Local security co-ordination
			Malware protection
			Management commitment
NW1.4 Network documentation NW5.1 Voice network documentation			Network documentation
			Outsourcing
			Patch management
NW3.4 Physical security		UE6.4 Physical and environmental protection	Physical protection

Topic	SM	CB	CI
Portable storage devices			
Post-implementation review			
Power supplies			CI2.7 Power supplies
Public key infrastructure	SM6.2 Public key infrastructure	CB6.3 Public key infrastructure	
Quality assurance			
Remote maintenance			
Remote working	SM6.4 Remote working		
Resilience		CB4.2 Resilience	CI2.5 Resilience
Roles and responsibilities	SM3.2 Ownership	CB2.1 Roles and responsibilities	CI1.1 Roles and responsibilities
Security architecture	SM4.1 Security architecture		
Security audit / review	SM7.1 Security audit / review	CB5.4 Security audit / review	CI5.5 Security audit / review
Security awareness	SM2.4 Security awareness	CB3.4 Security awareness	CI5.2 Security awareness
Security education / training	SM2.5 Security education / training		
Security event logging			CI2.2 Security event logging
Security monitoring	SM7.2 Security monitoring		
Service providers		CB4.1 Service agreements	CI1.2 Service agreements
Sign-on process		CB3.2 Application sign-on process	CI4.4 Sign-on process
Special controls			

NW	SD	UE	Topic
		UE4.3 Portable storage devices	Portable storage devices
	SD6.3 Post-implementation review		Post-implementation review
			Power supplies
			Public key infrastructure
	SD1.3 Quality assurance		Quality assurance
NW3.7 Remote maintenance			Remote maintenance
			Remote working
NW1.3 Network resilience NW5.2 Resilience of voice networks			Resilience
NW1.1 Roles and responsibilities	SD1.1 Roles and responsibilities	UE1.1 Roles and responsibilities	Roles and responsibilities
			Security architecture
NW4.5 Security audit / review	SD2.3 Security audit / review		Security audit / review
NW4.2 Security awareness	SD2.2 Security awareness	UE1.2 Security awareness	Security awareness
		UE1.3 User training	Security education / training
			Security event logging
			Security monitoring
NW1.5 Service providers			Service providers
		UE2.2 Application sign-on process	Sign-on process
NW5.3 Special voice network controls			Special controls

Topic	SM	CB	CI
Specifications of requirements			
Staff agreements	SM1.3 Staff agreements		
System design / build			
System / network monitoring			CI1.4 System monitoring
System promotion criteria			
Testing			
Third party access	SM6.5 Third party access	CB6.1 Third party agreements	
User authentication			CI4.5 User authentication
User authorisation			CI4.2 User authorisation
Voice over IP (VoIP) networks			
Web-enabled applications		CB6.4 Web-enabled applications	
Wireless access			
Workstation protection		CB3.3 Workstation protection	CI2.4 Workstation protection

NW	SD	UE	Topic
	SD3.1 Specification of requirements		Specifications of requirements
			Staff agreements
	SD4.1 System design SD4.5 System build		System design / build
NW3.1 Network monitoring			System / network monitoring
	SD6.1 System promotion criteria		System promotion criteria
	SD5.1 Testing process SD5.2 Acceptance testing		Testing
			Third party access
			User authentication
			User authorisation
NW5.4 Voice over IP (VoIP) networks		UE5.5 Voice over IP (VoIP) networks	Voice over IP (VoIP) networks
	SD4.6 Web-enabled development		Web-enabled applications
NW2.4 Wireless access		UE5.6 Wireless access	Wireless access
		UE4.1 Workstation protection	Workstation protection

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

Security Management (Enterprise-wide)

Keeping the business risks associated with information systems under control within an organisation requires clear direction and commitment from the top, the allocation of adequate resources, effective arrangements for promoting good information security practice throughout the organisation and the establishment of a secure environment.

Security Management

SM1 High-level Direction

SM1.1 Management commitment

SM1.2 Information security policy

SM1.3 Staff agreements

SM2 Security Organisation

SM2.1 High-level control

SM2.2 Information security function

SM2.3 Local security co-ordination

SM2.4 Security awareness

SM2.5 Security education / training

SM3 Security Requirements

SM3.1 Information classification

SM3.2 Ownership

SM3.3 Managing information risk analysis

SM3.4 Information risk analysis methodologies

SM3.5 Legal and regulatory compliance

SM4 Secure Environment

SM4.1 Security architecture

SM4.2 Information privacy

SM4.3 Asset management

SM4.4 Identity and access management

SM4.5 Physical protection

SM4.6 Information security incident management

SM4.7 Business continuity

SM5 Malicious Attack

SM5.1 General malware protection

SM5.2 Malware protection software

SM5.3 Intrusion detection

SM5.4 Emergency response

SM5.5 Forensic investigations

SM5.6 Patch management

SM6 Special Topics

SM6.1 Cryptographic solutions

SM6.2 Public key infrastructure

SM6.3 E-mail

SM6.4 Remote working

SM6.5 Third party access

SM6.6 Electronic commerce

SM6.7 Outsourcing

SM6.8 Instant messaging

SM7 Management Review

SM7.1 Security audit / review

SM7.2 Security monitoring

Area SM1
HIGH-LEVEL DIRECTION

Achieving an effective and consistent standard of good practice for information security throughout the organisation requires clear direction from the top. Accordingly, this area covers top management's direction on, and commitment to, information security. It specifies an information security policy and a set of staff agreements that should be applied to all individuals who have access to the information and systems of the organisation.

Section SM1.1 Management commitment

Principle Top management's direction on information security should be established, and commitment demonstrated.

Objective To ensure an appropriate set of security controls is implemented enterprise-wide.

SM1.1.1

Top management (eg board-level executives or equivalent) should have a high level of commitment to:

a) achieving high standards of corporate governance, such as those required by the Hampel combined code (UK), King II (RSA), Sarbanes-Oxley Act (USA) and the Commonwealth Association of Corporate Governance principles
b) treating information security as a critical business issue
c) creating a security-positive environment
d) demonstrating to third parties that the organisation deals with information security in a professional manner.

SM1.1.2

Top management should have a high level of commitment to applying fundamental principles, which include:

a) assuming ultimate responsibility for the internal controls of the organisation
b) ensuring that controls over information and systems are proportionate to risk
c) assigning responsibility for identifying, classifying and safeguarding information and systems to individual owners
d) granting access to information and systems in accordance with explicit criteria.

SM1.1.3

Top management should demonstrate their commitment to information security by:

a) assigning overall responsibility for information security to a board-level executive or equivalent (eg a Chief Information Security Officer)
b) chairing key information security working groups, committees or equivalent
c) monitoring the information security condition of the organisation
d) allocating sufficient resources (eg funding and staff) to information security.

SM1.1.4

Top management should demonstrate commitment by signing off high-level documentation, which includes the:

a) strategy for information security
b) information security policy
c) security architecture for the organisation.

Section SM1.2 Information security policy

Principle A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the organisation's information and systems.

Objective To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

SM1.2.1

There should be a documented information security policy, ratified at board level, that applies across the organisation. There should be an individual (or a group of individuals) responsible for maintaining the policy.

SM1.2.2

The information security policy should define information security, associated responsibilities and the information security principles to be followed by all staff.

SM1.2.3

The information security policy should require that:

a) information is classified in a way that indicates its importance to the organisation
b) owners (typically the people in charge of business processes that are dependent on information and systems) are appointed for all critical information and systems
c) important information and systems be subject to an information risk analysis on a regular basis
d) staff are made aware of information security
e) compliance with software licenses and with other legal, regulatory and contractual obligations is met
f) breaches of the information security policy and suspected information security weaknesses are reported
g) information is protected in terms of its requirements for confidentiality, integrity and availability.

SM1.2.4

The information security policy should be:

a) aligned with other high-level policies (eg those relating to human resources, health and safety, finance and information technology)
b) communicated to all staff and external individuals with access to the organisation's information or systems
c) reviewed regularly according to a defined review process
d) revised to take account of changing circumstances (eg new threats, vulnerabilities and risks, reorganisation of the organisation, changes to contractual, legal and regulatory requirements, or changes to the IT infrastructure).

SM1.2.5

The information security policy should:

a) be supported by methods to assess compliance (eg by checking if information risk analyses have been conducted, adherence to a patch management process, and verifying the configuration of security controls that have been applied to applications and systems)
b) state that disciplinary actions may be taken against individuals who violate its provisions.

SM1.2.6

A high-level policy (eg the information security policy) should instruct users to:

a) lock away sensitive media or documentation when not in use (ie complying with a 'clear desk' policy)
b) log off or lock systems if leaving a terminal unattended (eg during a meeting, lunch break or overnight).

(continued on the next page)

Section SM1.2 Information security policy (continued)

SM1.2.7

A high-level policy (eg the information security policy) should prohibit:

a) unauthorised use of the organisation's information and systems
b) using information and systems for purposes that are not work-related
c) making sexual, racist or other statements that may be offensive (eg when using e-mail, instant messaging, the Internet, or the telephone)
d) making obscene, discriminatory or harassing statements, which may be illegal (eg when using e-mail, instant messaging, the Internet, or the telephone)
e) downloading illegal material (eg with obscene or discriminatory content)
f) the movement of information or equipment off-site without authorisation
g) using unauthorised information facilities or equipment (eg unauthorised third party software, USB sticks or modems)
h) unauthorised copying of information or software
i) compromising passwords (eg by writing them down or disclosing them to others)
j) using personally identifiable information (ie information that can be used to identify an individual person) unless explicitly authorised
k) discussing business information in public places (eg train carriages, airport lounges or bars)
l) tampering with evidence in the case of information security incidents that may require forensic investigation.

Section SM1.3 Staff agreements

Principle Staff agreements should be established that specify information security responsibilities, are incorporated into staff contracts, and are taken into account when screening applicants for employment.

Objective To ensure that staff behave in a manner that supports the organisation's information security policy.

SM1.3.1

Information security responsibilities for all staff enterprise-wide should be specified in job descriptions and in terms and conditions of employment (eg in a contract or employee handbook).

SM1.3.2

Terms and conditions of employment should:

a) state that information security responsibilities extend outside normal working hours and premises, and continue after employment has ended
b) explain the employee's legal responsibilities and rights (eg regarding copyright laws or data protection)
c) include a non-disclosure / confidentiality clause.

SM1.3.3

There should be a requirement for staff to accept terms and conditions of employment in writing, and external individuals (eg consultants, contractors and employees of third parties) to sign non-disclosure / confidentiality agreements.

SM1.3.4

There should be a documented requirement for access privileges to be revoked immediately when an authorised user no longer requires access to information or systems as part of their job, or when they leave the organisation.

SM1.3.5

Applicants for employment (including internal staff and external individuals such as consultants, contractors and employees of third parties) should be screened prior to commencing work (eg by taking up references, checking career history / qualifications and confirming identity by inspecting a passport).

SM1.3.6

Key staff documents, such as policies or job descriptions, should be reviewed by an information security specialist, signed off by top management (eg a board-level executive, or equivalent) and kept up-to-date.

SM1.3.7

Upon termination of employment, staff and external individuals should be required to document information related to processes that are critical to the success of the organisation, and return:

a) equipment that belongs to the organisation
b) important information in electronic or paper form
c) software
d) authentication hardware (eg smartcards and tokens).

Area SM2

SECURITY ORGANISATION

Safeguarding information and systems requires information security activity to be organised effectively throughout the organisation. Accordingly, this area covers the organisational arrangements for managing information security throughout the organisation, raising security awareness amongst staff and ensuring they have the skills required to run systems correctly and securely.

Section SM2.1 High-level control

Principle Control over information security should be provided by a high-level working group, committee or equivalent body, and be supported by a top-level executive.

Objective To provide a top-down management structure and a practical mechanism for co-ordinating information security activity throughout the organisation.

SM2.1.1

There should be a top-level executive (or equivalent) with overall responsibility for information security.

SM2.1.2

A high-level working group, committee or equivalent body should be established for co-ordinating information security activity across the organisation. The group should meet on a regular basis (eg three or more times a year) and document actions agreed at meetings.

SM2.1.3

Membership of the high-level working group should include:

a) top management (ie a board-level executive or equivalent)
b) one or more business owners (ie people in charge of particular business applications or processes)
c) the head of information security, or equivalent (eg the Chief Information Security Officer)
d) representatives of other security-related functions (eg legal, operational risk, internal audit, insurance, human resources, and physical security)
e) the head of IT (or equivalent).

SM2.1.4

The high-level working group should be responsible for:

a) considering information security enterprise-wide
b) ensuring information security is addressed in a consistent, coherent manner
c) approving information security policies and standards / procedures
d) monitoring the organisation's exposure to information security threats
e) monitoring information security performance (eg analysing the current security status, handling information security incidents and costs)
f) approving and prioritising information security improvement activity
g) ensuring information security is addressed in the organisation's IT planning process
h) emphasising the importance of information security to the organisation.

Section SM2.2 Information security function

Principle A specialist information security function should be established, which has responsibility for promoting information security enterprise-wide.

Objective To ensure good practice in information security is applied effectively and consistently throughout the organisation.

SM2.2.1

The organisation should be supported by an information security function (or equivalent), which has responsibility for promoting good practice in information security enterprise-wide. The head of the information security function should be dedicated to information security full-time.

SM2.2.2

The information security function should:

a) develop and maintain an information security strategy
b) co-ordinate information security across the organisation
c) define a set of security services (eg identity services, authentication services, cryptographic services), which provide a coherent range of security capabilities
d) develop information security standards / procedures and guidelines
e) provide expert advice on all aspects of information security (eg information risk analysis, information security incident management and malware protection)
f) oversee the investigation of information security incidents
g) run one or more information security awareness programmes and develop security skills for staff enterprise-wide
h) evaluate the security implications of specialised business initiatives (eg outsourcing, electronic commerce initiatives and information exchange)
i) monitor the effectiveness of information security arrangements (eg using tools such as the ISF's FIRM, ROSI and Security Healthcheck).

SM2.2.3

The information security function should provide support for:

a) information risk analysis activities
b) important security-related projects
c) major IT projects with security requirements
d) security audits / reviews
e) classification of information and systems according to their importance to the organisation
f) the use of cryptography
g) incorporating information security requirements into documented agreements (eg contracts or service level agreements)
h) the development of business / service continuity plans.

(continued on the next page)

Section SM2.2 Information security function (continued)

SM2.2.4

The information security function should monitor:

a) general business trends (eg prospects for growth, internationalisation, electronic commerce and outsourcing)
b) technological developments (eg web-based technology, service oriented architecture (SOA) and Voice over IP)
c) new and emerging threats (eg identity theft, spear phishing and Bluetooth attacks)
d) new vulnerabilities in key operating systems, applications and other software (eg using vendor websites and mailing lists)
e) new information security solutions (eg digital rights management and intrusion prevention)
f) emerging industry / international information security-related standards (eg the Standard of Good Practice, ISO/IEC 27002 (17799), and COBIT v4.1)
g) emerging legislation or regulations related to information security (eg those related to data privacy, digital signatures and industry-specific standards such as Basel II 1998 and the Payment Card Industry (PCI) Data Security Standard).

SM2.2.5

The information security function should:

a) be adequately resourced in terms of the number of staff, their range and level of skills, and tools or techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture)
b) have sufficient impact on the organisation and strong support from top management, other business managers and IT managers
c) maintain contact with counterparts in the commercial world, government and law enforcement agencies and with security experts in computer / software companies and service providers
d) be reviewed on a regular basis (eg to ensure it performs as expected).

Section SM2.3 Local security co-ordination

Principle Arrangements should be made to co-ordinate information security activity in individual business units / departments.

Objective To ensure that security activities are carried out in a timely and accurate manner, enterprise-wide, and that security issues are resolved effectively.

SM2.3.1

Responsibility for information security should be assigned to the individual in charge of each major business unit or department.

SM2.3.2

Local information security co-ordinators should be appointed to co-ordinate information security throughout the organisation, including for business applications, computer installations, network environments, system development activities and end user environments.

SM2.3.3

Local information security co-ordinators should have:

a) a clear understanding of their roles and responsibilities
b) sufficient technical skills, time, necessary tools (eg checklists and specialist software products) and authority to carry out their assigned roles
c) access to in-house or external expertise in information security
d) documented standards / procedures to support day-to-day information security activities
e) up-to-date information on issues and techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture) related to information security.

SM2.3.4

Information about the security condition of the organisation should be:

a) reported to the head of the information security function
b) presented in a consistent manner, on a regular basis.

Section SM2.4 Security awareness

Principle Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the organisation.

Objective To ensure all relevant individuals apply security controls and prevent important information used throughout the organisation from being compromised or disclosed to unauthorised individuals.

SM2.4.1

Specific activities should be performed to promote security awareness enterprise-wide. These activities should be:

a) endorsed by top management
b) the responsibility of a particular individual, organisational unit, working group or committee
c) supported by a documented set of objectives
d) delivered as part of an on-going security awareness programme
e) subject to project management disciplines
f) kept up-to-date with current practices and requirements
g) based on the results of a documented information risk analysis
h) aimed at reducing the frequency and magnitude of information security incidents
i) measurable.

Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities.

SM2.4.2

Security awareness should be promoted:

a) to top management, business representatives, IT staff and external individuals
b) be provided with information security education / training (eg using techniques such as presentations and computer-based training (CBT))
c) by supplying specialised security awareness material, such as brochures, reference cards, posters and intranet-based electronic documents.

SM2.4.3

Staff should be provided with guidance to help them understand:

a) the meaning of information security (ie the protection of the confidentiality, integrity and availability of information)
b) the importance of complying with information security policies and applying associated standards / procedures
c) their personal responsibilities for information security (eg reporting actual and suspected information security incidents).

SM2.4.4

The effectiveness of security awareness should be monitored by:

a) measuring the level of information security awareness of staff
b) reviewing the level of information security awareness regularly
c) measuring the benefits of security awareness activities (eg by monitoring the frequency and magnitude of information security incidents experienced).

(continued on the next page)

Section SM2.4 Security awareness (continued)

SM2.4.5

Security-positive behaviour should be encouraged by:

a) making attendance at security awareness training compulsory
b) publicising security successes and failures throughout the organisation
c) linking security to personal performance objectives / appraisals.

Section SM2.5 Security education / training

Principle Staff should be educated / trained in how to run systems correctly and how to develop and apply information security controls.

Objective To provide staff with the skills required to protect systems and fulfil their information security responsibilities.

SM2.5.1

Education / training should be given to provide staff with the skills they need to:

a) assess security requirements
b) propose information security controls
c) ensure that security controls function effectively in the environments in which they are applied.

SM2.5.2

Education / training should be given to provide business users with the skills they need to:

a) use systems correctly
b) apply information security controls.

SM2.5.3

Education / training should be given to provide IT and systems development staff with the skills they need to:

a) design systems and develop security controls in a disciplined manner
b) implement information security controls
c) run computer installations correctly and apply required security controls effectively
d) run networks correctly and apply required security controls effectively.

SM2.5.4

Education / training should be provided to enable information security specialists to:

a) understand the business environment
b) run security-related projects
c) communicate effectively (eg making presentations, facilitating meetings or influencing management)
d) perform specialist security activities (eg information risk analysis, forensic investigations and business continuity planning).

Area SM3

SECURITY REQUIREMENTS

Ensuring that the safeguards applied to information and systems are proportionate to their importance to the business is a fundamental element of good practice. Accordingly, this area covers arrangements for classifying critical information and systems, assigning ownership, managing information risk analysis, undertaking information risk analysis and legal and regulatory compliance.

Section SM3.1 Information classification

Principle An information classification scheme should be established that applies throughout the organisation, based on the confidentiality of information in use.

Objective To determine the level of protection that should be applied to particular types of information, thereby preventing unauthorised disclosure.

SM3.1.1

There should be an information classification scheme that applies across the organisation, which should:

a) take account of the potential business impact from the loss of confidentiality of information
b) be used to determine varying levels of confidentiality of information (eg top secret, company-in-confidence and public).

When classifying information, some organisations also take into account requirements for integrity (ie the need for information to be valid, accurate and complete) and availability (ie the need for information to be accessible when required).

SM3.1.2

An information classification scheme should be established to classify:

a) information stored in paper form (eg contracts, plans and system documentation held in hard copy form)
b) information stored in electronic form (eg files created using spreadsheet and database programs, word processors and presentation packages)
c) electronic communications (eg messages sent via e-mail, instant messaging).

SM3.1.3

The information classification scheme should require:

a) that information is protected in line with its information classification
b) 'sign off' of the assigned classification applied to information (eg top secret, company-in-confidence and public) by the relevant business owner
c) that information classifications are reviewed and updated regularly and when changes are made.

SM3.1.4

The information classification scheme should:

a) provide guidance on handling requirements for each classification (eg when copying, storing, and destroying information)
b) explain how to resolve conflicting classifications.

(continued on the next page)

Section SM3.1 Information classification (continued)

SM3.1.5

The information classification scheme should apply to information associated with:

a) business applications
b) computer installations
c) networks
d) systems under development
e) end user environments.

SM3.1.6

There should be approved methods for labelling classified:

a) information stored in paper form (eg using rubber ink stamps, adhesive labels, hologram lamination)
b) information stored in electronic form (eg using electronic watermarking, labelling headers and footers, using filename conventions)
c) electronic communications (eg using digital signatures and clearly identifying the classification in the subject headers of e-mails).

SM3.1.7

An inventory (or equivalent) of information classification details should be maintained (eg in a database, via a specialised piece of software, or on paper).

SM3.1.8

Information classification details recorded should include:

a) the classification of the information
b) the identity of the information owner
c) a brief description of the information classified.

Section SM3.2 Ownership

Principle Ownership of critical information and systems should be assigned to capable individuals, with responsibilities clearly defined and accepted.

Objective To achieve individual accountability for the protection of all critical information and systems throughout the organisation.

SM3.2.1

Ownership of critical information and systems should be assigned to individuals, and the responsibilities of owners documented. Responsibilities for protecting information and systems should be communicated to owners and accepted by them.

SM3.2.2

Responsibilities of owners should include:

a) determining business (including information security) requirements and signing them off
b) ensuring information and systems are protected in line with their importance to the organisation
c) defining information interchange agreements (or equivalent)
d) developing service level agreements (SLAs)
e) authorising new or significantly changed systems
f) being involved in security audits / reviews.

SM3.2.3

The responsibilities of owners should involve:

a) determining which users are authorised to access particular information and systems
b) signing off access privileges for each user or set of users
c) ensuring users are aware of their security responsibilities and are able to fulfil them.

SM3.2.4

A process should be established for:

a) providing owners with the necessary skills, tools, staff and authority to fulfil their responsibilities
b) assigning responsibilities for protecting information and systems when the owner is unavailable
c) reassigning ownership when an owner leaves or changes roles.

Section SM3.3 Managing information risk analysis

Principle Critical business applications, computer installations, networks and systems under development should be subject to information risk analysis on a regular basis.

Objective To enable individuals who are responsible for critical information and systems to identify key information risks and determine the controls required to keep those risks within acceptable limits.

SM3.3.1

Decision-makers (including top management; heads of business units / departments; and owners of business applications, computer installations, networks, systems under development and end user environments) should be aware of the need to apply information risk analysis to critical environments within the organisation.

SM3.3.2

There should be documented standards / procedures for performing information risk analysis, which apply across the organisation. Documented standards / procedures should require risks to be analysed for:

a) information and systems that are important to the organisation
b) systems at an early stage in their development
c) systems subject to significant change, at an early stage in the change process
d) the introduction of major new technologies (eg wireless networks, instant messaging and Voice over IP)
e) requests to permit access from external locations (eg employees' homes, third party premises or public places)
f) requests to permit access to the organisation's information and systems by external individuals (eg consultants, contractors and employees of third parties).

SM3.3.3

Standards / procedures should specify that information risk analysis:

a) be performed regularly
b) involve business owners, IT specialists, key user representatives and experts in information risk analysis and information security specialists.

SM3.3.4

The results from information risk analyses that are conducted across the organisation should be:

a) reported to top management
b) used to help determine programmes of work in information security (eg remedial action and new security initiatives)
c) integrated with wider risk management activities (eg managing operational risk).

Section SM3.4 Information risk analysis methodologies

Principle Information risk analysis conducted on applications, computer installations, networks and systems under development should be undertaken using structured methodologies.

Objective To ensure information risk analysis is conducted in a consistent, rigorous and reliable manner throughout the organisation.

SM3.4.1

Risks associated with the organisation's information and systems should be analysed using structured information risk analysis methodologies (eg the ISF's Information Risk Analysis Methodology (IRAM)).

SM3.4.2

Information risk analysis methodologies should be:

a) documented
b) approved by top management
c) consistent across the organisation
d) automated (eg using specialist software tools)
e) reviewed regularly to ensure that they meet business needs
f) applicable to systems of various sizes and types
g) understandable to relevant business representatives.

SM3.4.3

Information risk analysis methodologies should require all risk analyses to have a clearly defined scope.

SM3.4.4

Information risk analysis methodologies should determine risk by assessing:

a) the potential level of business impact associated with the system, network or computer installation
b) deliberate threats to the confidentiality, integrity and availability of information and systems (eg carrying out denial of service attacks, malware, installing unauthorised software, misusing systems to commit fraud)
c) accidental threats to the confidentiality, integrity and availability of information and systems (eg loss of power, system or software malfunctions)
d) vulnerabilities due to control weaknesses
e) vulnerabilities due to circumstances that increase the likelihood of a serious information security incident occurring (eg use of the Internet, permitting third party access or siting a computer installation in an area prone to earthquakes or flooding).

SM3.4.5

Information risk analysis methodologies should take into account:

a) compliance requirements (eg with legislation, regulation, contractual terms, industry standards and internal policies)
b) objectives of the organisation
c) information classification requirements
d) previous risk analyses conducted on the application, network or computer installation being assessed
e) characteristics of the operating environment of the application, network or computer installation being assessed.

(continued on the next page)

Section SM3.4 Information risk analysis methodologies (continued)

SM3.4.6

Information risk analysis methodologies should ensure that the results of the information risk analysis are documented and include:

a) a clear identification of key risks
b) an assessment of the potential business impact of each risk
c) recommended actions to reduce risk to an acceptable level.

SM3.4.7

Information risk analysis methodologies should be used to help:

a) select security controls that will reduce the likelihood of serious information security incidents occurring
b) select security controls that will satisfy relevant compliance requirements (eg those outlined in the Sarbanes-Oxley Act 2002, the Payment Card Industry (PCI) Data Security Standard, Basel II 1998, data privacy requirements and anti-money laundering requirements)
c) evaluate the strengths and weaknesses of security controls
d) determine the costs of implementing security controls (eg costs associated with: design, purchase, implementation and monitoring of the controls; hardware and software; training; overheads, such as facilities; and consultancy fees)
e) identify specialised security controls required by particular environments (eg data encryption or strong authentication).

SM3.4.8

Information risk analysis methodologies should ensure that the results of the risk analysis (including risk treatment actions and any identified residual risk) are:

a) communicated to the relevant owner
b) signed off by the relevant owner
c) compared with information risk analyses conducted in other areas of the organisation.

Risk treatment typically involves one of four options: applying appropriate controls; accepting risks; avoiding risks; or transferring risks. Residual risk is that proportion of risk that still remains after selected controls have been implemented.

Section SM3.5 Legal and regulatory compliance

Principle A process should be established to identify and interpret the information security implications of relevant laws and regulations.

Objective To comply with laws and regulations affecting information security.

SM3.5.1

Legal and regulatory requirements affecting information security should be recognised by:

a) top management
b) one or more business owners
c) the head of information security (or equivalent)
d) representatives of other security-related functions (eg legal, operational risk, internal audit, insurance, human resources, and physical security).

SM3.5.2

A process should be established for ensuring compliance with relevant legal and regulatory requirements affecting information security, which covers:

a) information security-specific legislation (eg computer crimes, electronic commerce, and encryption export)
b) general legislation which has security implications (eg data privacy, investigatory powers, intellectual property, and human rights)
c) regulation (eg financial regulation, anti-money laundering, corporate governance, healthcare and industry specific regulations such as the Payment Card Industry (PCI) Data Security Standard and HIPAA).

SM3.5.3

The compliance process should enable decision-makers to:

a) discover laws and regulations that affect information security
b) interpret the information security implications of these laws and regulations
c) identify potential legal / regulatory non-compliance (eg performing a risk analysis of compliance with laws and regulations)
d) address areas of potential legal / regulatory non-compliance.

SM3.5.4

The compliance process should be documented, signed off by top management, and kept up-to-date.

SM3.5.5

A review of compliance with legal and regulatory requirements that affect information security should be:

a) performed regularly or when new legislation or regulatory requirements come into effect
b) conducted by representatives from key areas of the organisation (eg top management, business owners, legal department, IT management, and the information security function).

SM3.5.6

Following the review of compliance with relevant legal and regulatory requirements, information security standards / procedures should be updated to accommodate any necessary changes.

Area SM4
SECURE ENVIRONMENT

Achieving a consistent standard of good practice in information security across an organisation is a complex undertaking. The difficulties can be eased by introducing a common framework of disciplines and by making standard arrangements at organisation level, rather than on an individual basis (eg by developing a security architecture, establishing identity and access arrangements, creating a capability for managing information security incidents, and planning business continuity for the whole organisation). Accordingly, this area covers the arrangements required to build a secure environment enterprise-wide.

Section SM4.1 Security architecture

Principle A security architecture should be established, which provides a framework for the application of standard security controls throughout the organisation.

Objective To enable system developers and administrators to implement consistent, simple-to-use security functionality across multiple computer systems throughout the organisation.

SM4.1.1

A security architecture should be established and incorporated into the organisation's enterprise architecture (or equivalent).

SM4.1.2

Development of the security architecture should involve:

a) an assessment of business security requirements
b) the use of a layered security architecture model (eg consisting of conceptual, logical and physical layers)
c) the definition of security architecture principles
d) the identification of security components that may be included in the security architecture (eg security controls, security services and security technologies)
e) the development of tools and resources that will be used to help manage the security architecture (eg repositories of solutions, design patterns, code samples and application programming interfaces (APIs)).

Security architecture principles (sometimes referred to as guiding principles or design principles) represent fundamental security rules that should be followed during the development of a security architecture for a system, and applied when the corresponding security controls are implemented.

Examples of security architecture principles include 'security by design', 'defence in depth', 'least privilege', 'default deny' and 'fail secure'.

SM4.1.3

Development of the security architecture should include:

a) input from relevant internal specialists (eg a security architect, technical architect or information security specialist)
b) use of an independent external security architecture specialist
c) education of individuals that need to use the security architecture (eg information security specialists, software developers and IT implementers)
d) introducing a method of measuring the uptake of the security architecture across the organisation.

(continued on the next page)

Section SM4.1 Security architecture (continued)

SM4.1.4

The security architecture should be applied to:

a) the development of business applications (eg to help manage complexity and scale, make effective design decisions, and improve the quality and security of business applications)
b) help manage the IT infrastructure (eg to help in the development of a secure IT infrastructure, and assist in the review and analysis of the existing IT infrastructure)
c) major IT projects (eg to help deal with complexity, new information risks and large scale environments).

SM4.1.5

The security architecture should be:

a) documented (eg in the form of blueprints, designs, diagrams, tables or models)
b) approved by business, IT and information security managers
c) assigned to an owner (eg a chief architect or a high-level working group, such as an Architecture Board, or equivalent)
d) maintained (eg involving reviews, exception handling and change management).

SM4.1.6

There should be an enterprise-wide process for implementing coherent and consistent security services (eg identity services, authentication services and cryptographic services) and establishing common user and application programming interfaces (APIs).

SM4.1.7

Arrangements should be made enterprise-wide to:

a) minimise the diversity of hardware / software in use
b) provide consistent security functionality across different hardware / software platforms
c) integrate security controls at application, computer and network level
d) apply consistent cryptographic techniques
e) implement common naming conventions
f) segregate environments with different security requirements (eg by creating 'trusted' and 'untrusted' security domains)
g) control the flow of information between different environments.

Section SM4.2 Information privacy

Principle Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.

Objective To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.

SM4.2.1

A high-level committee (or equivalent) should be established to be responsible for managing information privacy issues, and an individual appointed to co-ordinate information privacy activity (eg a Chief Privacy Officer or a Data Protection Manager).

SM4.2.2

The high-level committee (or equivalent) should be aware of:

a) the location(s) of personally identifiable information held about individuals
b) how and when personally identifiable information is used.

SM4.2.3

There should be documented standards / procedures for dealing with information privacy, which cover:

a) acceptable use of personally identifiable information
b) the rights of individuals about whom personally identifiable information is held
c) privacy assessment, awareness and compliance programmes
d) legal and regulatory requirements for privacy.

SM4.2.4

Where personally identifiable information is stored or processed, there should be processes to ensure that it is:

a) adequate, relevant and not excessive for the purposes for which it is collected
b) accurate (ie recorded correctly and kept up-to-date)
c) kept confidential, processed fairly and legally, and used only for specified, explicit and legitimate purposes
d) held in a format that permits identification of individuals for no longer than is necessary
e) only provided to third parties that can demonstrate compliance with legal and regulatory requirements for handling personally identifiable information
f) retrievable in the event of a legitimate request for access.

SM4.2.5

Individuals about whom personally identifiable information is held (eg the 'data subject' according to the EU Directive on Data Protection) should:

a) have their approval sought before this information is collected, stored, processed or disclosed to third parties
b) be informed of how this information will be used, allowed to check its accuracy and able to have their records corrected or removed.

SM4.2.6

Personally identifiable information should be handled in accordance with relevant legislation (eg the EU Directive on Data Protection or the US Health Insurance Portability and Accounting Act (HIPAA)).

(continued on the next page)

Section SM4.2 Information privacy (continued)

SM4.2.7

An individual (or group) within the organisation should:

a) perform a privacy assessment (eg to determine the level of compliance with relevant legislation and internal policies)
b) implement a privacy compliance programme
c) make staff and third parties (eg customers, clients and suppliers) aware of the importance of information privacy.

Section SM4.3 Asset management

Principle Proven, reliable and approved hardware / software should be used that meet security requirements and are recorded in an inventory.

Objective To reduce the risk of information security being compromised by weaknesses in hardware / software.

SM4.3.1

There should be documented standards / procedures for asset management, which cover:

a) acquisition of software / hardware
b) software licensing
c) recording of assets in an inventory (or equivalent)
d) archiving of important information.

SM4.3.2

When acquiring hardware / software:

a) they should be selected from a list of approved suppliers
b) security requirements should be considered
c) high priority should be given to reliability
d) contractual terms should be agreed with suppliers.

SM4.3.3

The risk of potential security weaknesses in hardware / software should be reduced by:

a) obtaining external assessments from trusted sources (eg auditors' opinions and specified security criteria, such as the 'Common Criteria' and FIPS (Federal Information Processing Standards))
b) identifying security deficiencies (eg by detailed inspection, reference to published sources, or by participating in user / discussion groups)
c) considering alternative methods of providing the required level of security (eg 'work-arounds').

SM4.3.4

The acquisition of hardware / software should be reviewed by staff who have the necessary skills to evaluate them, and be approved by an appropriate business representative.

SM4.3.5

Software licensing requirements should be met by obtaining adequate licenses for planned use and by providing proof of ownership of software (eg via 'blanket' licence agreements).

SM4.3.6

Hardware / software (including critical desktop applications) should be recorded in inventories, such as asset registers or equivalent, which specify a unique description of hardware / software in use, together with its version and location.

(continued on the next page)

Section SM4.3 Asset management (continued)

SM4.3.7

Hardware / software inventories (or equivalent) should be:

a) protected against unauthorised change
b) checked regularly against physical assets
c) kept up-to-date
d) reviewed independently.

SM4.3.8

Important information should be retained in accordance with legal / regulatory requirements (eg by archiving it to removable media and storing in a safe location).

Section SM4.4 Identity and access management

Principle Identity and access management arrangements should be established to provide effective and consistent user administration, identification, authentication and access mechanisms across the organisation.

Objective To restrict system access to authorised users and ensure the integrity of important user information.

SM4.4.1

Identity and access management arrangements should be established to provide enterprise-wide user provisioning and access control.

Identity and access management (IAM) typically consists of a number of discrete activities that follow the stages of a user's life cycle within the organisation. These activities fall into two categories, which are the:

- provisioning process, which provides users with the user accounts and access rights they require to access systems and applications
- user access process, which relates to the actions performed each time a user attempts to access a new system, such as authentication and sign-on.

SM4.4.2

IAM arrangements should be incorporated into an enterprise-wide solution, and applied to new business applications when they are introduced into the organisation.

SM4.4.3

IAM arrangements should:

a) include a method for validating user identities prior to enabling user accounts
b) keep the number of sign-ons required by users to a minimum (ie reduced or single sign-on).

SM4.4.4

IAM arrangements should provide a consistent set of methods for:

a) identifying users (eg using unique UserIDs)
b) authenticating users (eg using passwords, tokens or biometrics)
c) the user sign-on process
d) authorising user access privileges
e) administering user access privileges.

SM4.4.5

IAM arrangements should be developed to improve the integrity of user information by:

a) making the information readily available for users to validate (eg by using an electronic information database or directory, such as white pages)
b) allowing users to correct their own user information (eg by providing users with a self-service application)
c) maintaining a limited number of identity stores (ie the location where UserID and authentication information is stored, such as a database, X500 / Lightweight Directory Access Protocol (LDAP) directory service, or commercial IAM product)
d) using an automated provisioning system (whereby user accounts are created for all target systems, following the creation of an initial entry for a user in a central IAM application)
e) using a centralised change management system.

(continued on the next page)

Section SM4.4 Identity and access management (continued)

SM4.4.6

IAM arrangements should enable:

a) access rights to be quickly and easily granted, changed or removed for a large number of users (eg by deploying role-based access rights)
b) management of user access privileges to be performed by relevant system owners (ie rather than by system administrators / IT staff).

Section SM4.5 Physical protection

Principle All locations that house critical IT facilities, sensitive material and other important assets should be physically protected against accident or attack.

Objective To restrict physical access to authorised individuals and ensure that critical IT facilities processing important information, sensitive material and other important assets are available when required.

SM4.5.1

There should be documented standards / procedures for the provision of physical protection in areas housing critical IT facilities within the organisation.

SM4.5.2

Standards / procedures should cover the protection of:

a) buildings against unauthorised access (eg by using locks, security guards and video surveillance)
b) important papers and removable storage media (eg CDs, DVDs and USB memory sticks) against theft or copying
c) storage areas (eg that might be used to store organisational assets, computer equipment and media, or important paper-based documents)
d) vulnerable staff against intimidation by malicious third parties.

SM4.5.3

Buildings that house critical IT facilities should be protected against unauthorised access by:

a) providing locks, bolts (or equivalent) on vulnerable doors and windows
b) employing security guards
c) installing closed-circuit television (CCTV), or equivalent.

SM4.5.4

Important papers and removable storage media (eg CDs, DVDs and USB memory sticks) should be protected against theft or copying by:

a) storing sensitive physical material in locked cabinets (or similar) when not in use (eg by enforcing a 'clear desk' policy)
b) restricting physical access to important post / facsimile points
c) locating equipment used for sensitive printed material in secure physical areas.

SM4.5.5

Staff should be protected against intimidation from malicious third parties by providing duress alarms in susceptible public areas and establishing a process for responding to emergency situations.

Section SM4.6 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

SM4.6.1

A capability for governing the management of information security incidents (ie event (or chains of events) that compromise the confidentiality, integrity or availability of information) should be established.

SM4.6.2

The information security incident management capability should be supported by documented standards / procedures, which:

a) cover the involvement of relevant stakeholders (eg legal department, public relations, human resources, law enforcement agencies, media and industry regulators)
b) detail the types of information needed to support information security incident management (eg security event log data, network configuration diagrams and information classification details)
c) specify the tools needed to support information security incident management (eg checklists, forms and templates, log analysers, incident tracking software and forensic analysis software).

SM4.6.3

Standards / procedures for information security incident management should be:

a) approved by top management (board-level executives or equivalent)
b) reviewed regularly
c) kept up-to-date.

SM4.6.4

There should be a process for managing individual information security incidents, which includes:

a) identifying information security incidents (eg receiving information security incident reports, assessment of business impact, categorisation and classification of the information security incident, and recording of information about the information security incident)
b) responding to information security incidents (eg escalation to the information security incident management team, investigation, containment and eradication of the cause of the information security incident)
c) recovering from information security incidents (eg rebuilding systems and restoring data, and closure of the information security incident)
d) following up information security incidents (eg post-incident activities such as root cause analysis, forensic investigation, and reporting to the business).

SM4.6.5

There should be a defined individual / team responsible for managing information security incidents, which have:

a) defined roles and responsibilities
b) sufficient skills / experience in managing information security incidents
c) authority to make critical business decisions
d) methods of involving internal and external stakeholders (eg legal department, public relations, human resources, law enforcement agencies, media and industry regulators).

(continued on the next page)

Section SM4.6 Information security incident management (continued)

SM4.6.6

Information relevant to managing information security incidents (eg network diagrams, event logs, business processes, and security audit reports) should be made available to help staff follow, and make important decisions during, the information security incident management process.

SM4.6.7

Individuals responsible for managing information security incidents should be supported by tools (eg software for security information management, evidence handling, back-up and recovery, and forensic investigation) to help complete each stage of the information security incident management process.

Section SM4.7 Business continuity

Principle Documented standards / procedures should be established for developing business continuity plans and for maintaining business continuity arrangements enterprise-wide.

Objective To enable the organisation to withstand the prolonged unavailability of critical information and systems.

SM4.7.1

There should be documented standards / procedures for developing business continuity plans, which specify that plans are:

a) provided for all critical parts of the organisation
b) based on the results of a documented information risk analysis
c) distributed to individuals who would require them in case of emergency
d) kept up-to-date and subject to standard change management practices
e) backed-up by copies stored off-site.

SM4.7.2

Business continuity plans should include:

a) guidelines to ensure the safety of individuals
b) a list of services and information to be recovered, in priority order
c) a schedule of tasks and activities to be carried out, identifying responsibilities for each task (including deputies)
d) guidelines to be followed in completing key tasks and activities, including emergency, fall-back and resumption procedures
e) sufficient detail so that they can be followed by individuals who do not normally carry them out
f) details of tasks to be undertaken following recovery and restoration (eg checking that the systems are restored to the same state they were in before the business continuity plan was invoked).

SM4.7.3

There should be documented standards / procedures for the provision of business continuity arrangements (eg separate processing facilities, reciprocal arrangements with another organisation or a contract with a specialist business continuity arrangements provider).

SM4.7.4

Business continuity arrangements should cover the prolonged unavailability of:

a) key individuals (eg due to illness, injury, vacation or travel)
b) office accommodation (eg due to police, military or terrorist action, natural disaster, or withdrawal of transport services)
c) systems or application software
d) business information (in paper or electronic form)
e) computer, communications and environmental control equipment
f) network services (eg due to loss of voice, data or other communications systems)
g) essential services (eg electricity, gas or water supplies).

SM4.7.5

Business continuity arrangements should cover critical:

a) business applications
b) IT facilities
c) business areas (eg trading floors, process control centres and call centres).

(continued on the next page)

Section SM4.7 Business continuity (continued)

SM4.7.6

Business continuity arrangements should be tested regularly, using realistic simulations (involving both users and IT staff), to demonstrate whether staff are capable of recovering critical information and systems within critical timescales.

SM4.7.7

Business continuity arrangements should require that relevant staff be informed of their business continuity responsibilities and trained to discharge them.

Area SM5

MALICIOUS ATTACK

Organisations are often subject to attack from malicious third parties (eg by sending malware or hacking systems). Consequently, this area covers the security controls required to protect against malware, keep applications and systems up-to-date with patches, provide intrusion detection capabilities, respond to a serious attack and manage forensic investigations.

Section SM5.1 General malware protection

Principle All individuals who have access to information and systems of the organisation should be made aware of the risks from malware, and the actions required to minimise those risks.

Objective To ensure all relevant individuals understand the key elements of malware protection, why it is needed, and help to keep the impact of malware to a minimum.

SM5.1.1

There should be documented standards / procedures covering protection against malware, which:

a) provide users with information about malware
b) warn users how to reduce the risk of malware infection.

Malware typically includes computer viruses, worms, trojan horses, spyware, adware and malicious mobile code (executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions).

SM5.1.2

Users should be:

a) warned of the prevalence of malware and the dangers it poses
b) educated about the ways in which malware can install itself on workstations
c) advised of the common symptoms of malware (eg poor system performance, unexpected application behaviour, sudden termination of an application)
d) notified quickly of significant new malware-related risks (eg by e-mail or via an intranet)
e) instructed to report suspected or actual malware to a single point of contact for support (eg a helpdesk or telephone hot line)
f) supported by specialist technical support at required times (eg 24 hours a day, 365 days a year).

SM5.1.3

The risk of malware infection should be reduced by warning users not to:

a) install software from untrusted sources
b) open untrusted attachments
c) click on hyperlinks within e-mails or documents
d) attempt to manually resolve malware problems.

(continued on the next page)

Section SM5.1 General malware protection (continued)

SM5.1.4

Malware protection should include:

a) implementing emergency procedures for dealing with malware-related information security incidents
b) monitoring external media sources for intelligence about new malware threats
c) informing third parties of the organisation's malware protection standards / procedures.

Section SM5.2 Malware protection software

Principle Effective malware protection software should be installed, configured, and maintained enterprise-wide.

Objective To protect the organisation against malware attacks and ensure malware infections can be addressed within defined timescales.

SM5.2.1

There should be documented standards / procedures related to malware protection software, which specify:

a) methods for installing and configuring malware protection software (eg virus protection software, anti-spyware software)
b) update mechanisms for malware protection software (including automatic updates).

SM5.2.2

Malware protection software should be installed on systems that are susceptible to malware (eg those that have access to the Internet), including:

a) relevant servers (eg servers that are at risk from malware, such as file and print servers, application servers, web servers and database servers)
b) messaging gateways (eg those that scan network traffic and electronic messages in real time)
c) desktop computers
d) laptop computers
e) hand-held computing devices (eg WAP-based mobile phones, smartphones and Personal Digital Assistants (PDA)).

SM5.2.3

Malware protection software should be distributed automatically, and within defined timescales to reduce the risk of systems being exposed to the most recent malware (including those that are associated with 'zero-day' attacks).

SM5.2.4

Malware protection software should protect against all forms of malware (eg computer viruses, worms, trojan horses, spyware, adware and malicious mobile code).

SM5.2.5

Malware protection software should be configured to scan:

a) computer memory
b) executable files (including macro files in desktop software)
c) protected files (eg compressed or password-protected files)
d) removable computer storage media (eg CDs, DVDs and USB storage devices)
e) network traffic entering the corporate network (including e-mail and downloads from the Internet)
f) network traffic leaving the corporate network (including e-mail).

(continued on the next page)

Section SM5.2 Malware protection software (continued)

SM5.2.6

Malware protection software should be configured to:

a) be active at all times
b) provide a notification when suspected malware is identified (eg by producing an event log entry and providing an alert)
c) quarantine files suspected to contain malware (eg for further investigation)
d) remove the malware and any associated files or reset system settings
e) ensure that important settings cannot be disabled or functionality minimised.

SM5.2.7

Regular reviews of servers, desktop computers, laptop computers and hand-held computing devices should be performed to ensure that:

a) malware protection software has not been disabled
b) the configuration of malware protection software is correct
c) updates are applied within defined timescales
d) emergency procedures are in place to deal with a malware-related information security incident.

SM5.2.8

The risk of downloading malware should be reduced by:

a) restricting the sources from which mobile code can be downloaded (eg by providing a blacklist of forbidden websites)
b) preventing the downloading of specific types of mobile code (eg those associated with known vulnerabilities, such as some ActiveX controls, JavaScript and Browser Helper objects)
c) configuring web browsers so that users are asked if they wish to install mobile code
d) allowing only trusted mobile code to be downloaded (ie signed with a trusted digital certificate)
e) running mobile code in a protected environment (eg a quarantine area such as a Java 'sandbox' or a proxy server in a 'Demilitarised Zone' (DMZ)).

Section SM5.3 Intrusion detection

Principle Intrusion detection mechanisms should be applied to critical systems and networks.

Objective To identify suspected or actual malicious attacks and enable the organisation to respond before serious damage is done.

SM5.3.1

Intrusion detection mechanisms should be employed for critical systems and networks to identify predetermined and new types of attack.

SM5.3.2

Intrusion detection methods should be supported by documented standards / procedures, which cover:

a) methods of identifying unauthorised activity
b) analysis of suspected intrusions
c) relevant responses to different types of attack (eg an information security incident management process).

SM5.3.3

Intrusion detection methods should identify:

a) unauthorised access (actual or attempted) to systems or information
b) unexpected user or application behaviour
c) unplanned termination of processes or applications
d) activity typically associated with malware.

SM5.3.4

Intrusion detection methods should be supported by specialist software, such as host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS). This software should be evaluated prior to purchase.

SM5.3.5

Network intrusion detection sensors (ie specialist hardware used to identify unauthorised activity in network traffic) should be protected against attack (eg by preventing the transmission of any outbound network traffic, or by using a network tap to hide the presence of the sensor).

SM5.3.6

Intrusion detection software should be:

a) updated automatically and within defined timescales (eg delivery of distribution attack signature files to intrusion detection sensors via a central management console)
b) configured to provide an alert when suspicious activity is detected (eg via a management console, e-mail messages or SMS text messages to mobile telephones).

SM5.3.7

Regular reviews should be performed to ensure that:

a) the configuration of intrusion detection software meets internal standards
b) intrusion detection software has not been disabled
c) updates have been applied within defined timescales.

(continued on the next page)

Section SM5.3 Intrusion detection (continued)

SM5.3.8

Suspected intrusions should be analysed and potential business impact assessed. Initial analysis should include:

a) confirming whether an attack is actually occurring (eg by eliminating false positives)
b) determining the type of attack (eg worms, buffer overflows or denial of service)
c) identifying the original point of an attack
d) quantifying the possible impact of an attack.

SM5.3.9

The status of an attack should be assessed in terms of:

a) time elapsed since the start of the attack and since detection of the attack
b) scale (eg particular systems and networks affected).

SM5.3.10

There should be a documented method (eg an escalation process) for reporting serious attacks (eg to an emergency response team).

Section SM5.4 Emergency response

Principle An emergency response process should be established, supported by an emergency response team, which outlines actions to be taken in the event of a serious attack.

Objective To respond to serious attacks quickly and effectively, reducing any potential business impact.

SM5.4.1

There should be an emergency response process for dealing with serious attacks.

SM5.4.2

The emergency response process should be supported by a predetermined high-level team (eg an emergency response team), which includes individuals skilled in responding to serious attacks, and a representative from top management.

SM5.4.3

There should be a process for dealing with serious attacks, which includes:

a) a definition of an emergency situation
b) allocation of roles and responsibilities
c) a defined method of enabling critical decisions to be made quickly
d) clearly defined steps to be taken in emergency situations
e) steps to be taken
f) contact details for all key individuals (including those associated with third parties)
g) methods of dealing with third parties (eg media, law enforcement agencies and security experts in computer / software companies).

SM5.4.4

The process should include methods of:

a) enabling investigators to react quickly should an emergency arise
b) gaining approval for recommended actions within a critical timescale.

SM5.4.5

The process should ensure that, after an emergency has occurred:

a) computers affected by the attack are cleaned (eg malicious programs and related files are removed from the computer)
b) the likelihood of similar attacks is minimised
c) security controls are reviewed.

Section SM5.5 Forensic investigations

Principle A process should be established for dealing with information security incidents that require forensic investigation.

Objective To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

SM5.5.1

A process should be established for dealing with information security incidents that may require forensic investigation.

SM5.5.2

There should be documented standards / procedures for dealing with information security incidents that may require forensic investigation, which cover:

a) immediate preservation of evidence on discovery of an information security incident (eg to support the need for a chain of custody to show who handled evidence from the time of discovery to the time of a court case)
b) compliance with a published standard or code of practice for the recovery of admissible evidence
c) maintenance of a log of evidence recovered and the investigation processes undertaken
d) the need to seek legal advice where evidence is recovered
e) actions that may be monitored during the investigation.

SM5.5.3

Evidence should be collected:

a) with the intention of possible legal action
b) with respect for individuals' privacy and human rights
c) from IT sources relevant to the information security incident (eg active, temporary and deleted files, e-mail or Internet usage, memory caches and network logs)
d) from non-IT sources relevant to the information security incident (eg CCTV recordings, building access logs and eye witness accounts).

SM5.5.4

During a forensic investigation steps should be taken to:

a) establish and document a chronological sequence of events
b) log investigative actions
c) demonstrate that appropriate evidence has been collected, preserved and that it has not been modified
d) protect target computer equipment against unauthorised access and tampering with possible evidence
e) analyse evidence in a controlled environment (eg using a copy or 'image' of the computer media to avoid corruption of the original)
f) have evidence reviewed by an impartial, independent expert to ensure that it meets legal / regulatory requirements
g) ensure that processes used to create and preserve evidence can be repeated by an independent third party
h) limit information about an investigation to a few nominated individuals and ensure it is kept confidential.

SM5.5.5

Results from a forensic investigation should be reported to relevant management (eg top management and heads of business units / departments) and appropriate legal / regulatory bodies.

Section SM5.6 Patch management

Principle A process should be established for the deployment of system and software patches.

Objective To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

SM5.6.1

There should be documented standards / procedures for patch management which specify the:

a) requirement to patch computer equipment, business applications, operating system / software and network components
b) organisation's approach to patching (eg what is to be patched)
c) testing requirements (eg provision of a test environment)
d) methods of patch distribution (eg automated deployment).

SM5.6.2

Standards / procedures for patch management should include a method of:

a) defining roles and responsibilities for patch management
b) determining the importance of systems (eg based on the information handled, the business processes supported and the environments in which they are used)
c) recording patches that have been applied (eg using an inventory of computer assets including their patch level).

SM5.6.3

A patch management process should be established to govern the application of patches on a day-to-day basis. The process should be documented, approved by relevant management, and assigned an owner.

SM5.6.4

The patch management process should:

a) determine methods of obtaining patches
b) specify methods of validating patches (eg ensuring that the patch is from an authorised source)
c) identify vulnerabilities that are applicable to applications and systems used by the organisation
d) assess the business impact of implementing patches (or not implementing a particular patch)
e) ensure patches are tested against known criteria
f) describe methods of deploying patches (eg using software distribution tools)
g) report on the status of patch deployment across the organisation
h) include methods of dealing with the failed deployment of a patch (eg redeployment of the patch).

SM5.6.5

Methods should be established to protect information and systems if no patch is available for an identified vulnerability (eg disabling services and adding additional access controls).

Area SM6
SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns that should be dealt with enterprise-wide. Accordingly, this area covers the special security controls that apply to the use of cryptography, public key infrastructure, electronic messaging, remote working, the provision of third party access, electronic commerce and outsourcing.

Section SM6.1 Cryptographic solutions

Principle Cryptographic solutions should be approved, documented and applied enterprise-wide.

Objective To protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of information.

SM6.1.1

Cryptography should be used across the organisation to:

a) protect the confidentiality of sensitive information (eg by using encryption)
b) determine if critical information has been altered (eg by performing hash functions)
c) provide strong authentication for users of applications and systems (eg by using digital certificates and smartcards)
d) enable the identity of the originator of critical information to be proven (eg by using digital signatures for non-repudiation).

SM6.1.2

There should be documented standards / procedures for the use of cryptography across the organisation, which cover the:

a) definition of circumstances where cryptography should be used (eg for high-value transactions involving external bodies or transmitting confidential information across open networks such as the Internet)
b) selection of approved cryptographic algorithms (eg Advanced Encryption Standard (AES) for confidentiality, and SHA-1 or MD5 for integrity)
c) management (including protection) of cryptographic keys
d) restrictions on the export / use of cryptographic solutions
e) suitability of cryptographic solutions employed (including algorithms and encryption key lengths).

SM6.1.3

Responsibilities should be clearly defined for managing cryptographic keys and dealing with licensing issues associated with the use of cryptographic solutions internationally.

SM6.1.4

Relevant business managers should have access to:

a) expert technical and legal advice on the use of cryptography
b) a list of approved cryptographic solutions
c) an up-to-date inventory (or equivalent) detailing where cryptographic solutions are applied within the organisation.

Section SM6.2 Public key infrastructure

Principle Where a public key infrastructure (PKI) is used, it should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.

Objective To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

SM6.2.1

For an organisation that makes use of a public key infrastructure (PKI), documented standards / procedures should be established, which define the:

a) process required to manage cryptographic keys / digital certificates within the PKI
b) methods required to operate the PKI
c) actions to be taken in the event of a compromise or suspected compromise of the PKI.

SM6.2.2

PKI users should be made aware of the purpose and function of the PKI, their responsibility to protect private keys, and how to use digital signatures.

SM6.2.3

A Certification Authority (CA) comprises the people, processes and tools that are responsible for the creation, issue and management of public key certificates that are used within a PKI. Where a PKI is supported by an internal CA, it should be protected by:

a) restricting access to authorised individuals (eg by using access control mechanisms and strong authentication)
b) 'hardening' the operating system(s) that support them (eg by removing all known vulnerabilities)
c) employing other general controls (eg change management) in a particularly disciplined manner.

SM6.2.4

Contingency plans for the application(s) supported by the PKI should include methods of recovering the PKI in the event of a disaster.

Section SM6.3 E-mail

Principle E-mail systems should be protected by a combination of policy, awareness, procedural and technical security controls.

Objective To ensure that e-mail services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

SM6.3.1

There should be documented standards / procedures for the provision and use of e-mail, which specify methods of:

a) configuring mail servers (eg to limit the size of messages or user mailboxes)
b) scanning e-mail messages (eg for malware, chain letters or offensive content)
c) enhancing the security of e-mail messages (eg by the use of disclaimers, hashing, encryption or non-repudiation techniques)
d) making users aware of the consequences of their actions when using e-mail.

SM6.3.2

Mail servers should be configured to prevent the messaging system being overloaded by limiting the size of messages / user mailboxes, restricting the use of large distribution lists and automatically identifying and cancelling e-mail loops.

SM6.3.3

E-mail systems should be reviewed to ensure that requirements for up-time and future availability can be met.

SM6.3.4

E-mail messages should be scanned for:

a) attachments that could contain malicious code (eg malicious code hidden in self-extracting zip files or MPEG video clips)
b) prohibited words (eg words that are racist, offensive, libellous or obscene)
c) phrases associated with malware (eg those commonly used in hoax viruses or chain letters).

SM6.3.5

E-mail systems should provide protection by:

a) blocking messages that are considered undesirable (eg by using an e-mail blacklist consisting of known undesirable websites or e-mail list servers)
b) using digital signatures to identify if e-mail messages have been modified in transit, and encrypting confidential or sensitive e-mail messages
c) ensuring non-repudiation of origin of important e-mail messages (eg by using digital signatures)
d) providing non-repudiation of receipt of important messages (eg by returning a digitally signed receipt message).

SM6.3.6

Business integrity should be protected by:

a) appending legally required information and return address details (for misdelivered e-mail) to business e-mail (eg as a disclaimer)
b) warning users that the contents of e-mail messages may be legally and contractually binding and that the use of e-mail may be monitored.

(continued on the next page)

Section SM6.3 E-mail (continued)

SM6.3.7

The organisation should prohibit:

a) the use of web-based e-mail
b) automatic e-mail diversion to external e-mail addresses
c) unauthorised advertising
d) private encryption of e-mail or attachments
e) the opening of attachments from unknown or untrusted sources.

SM6.3.8

Personal use of business e-mail should be clearly labelled as personal and subject to the terms of a user agreement.

Section SM6.4 Remote working

Principle Personal computers used by staff working in remote locations should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical and logical controls.

Objective To ensure that computers used by staff working in remote locations operate as intended, remain available and do not compromise the security of any facilities to which they can be connected.

SM6.4.1

Remote working should be supported by documented standards / procedures, which cover:

a) security requirements associated with remote working
b) the types of device that can be used by staff working in remote locations (eg laptop computers, hand-held computing devices, and smartphones)
c) implementation and maintenance of remote equipment
d) provision of software to protect workstations (eg system management tools, access control mechanisms, malware protection software and encryption capabilities)
e) software configuration (eg employing standard 'builds' and relevant web browser settings)
f) protection against malicious mobile code (eg Java applets, ActiveX, JavaScript or VBScript that have been written deliberately to perform unauthorised functions)
g) authorisation by an appropriate business representative for staff to work remotely.

SM6.4.2

Staff working in remote locations should be supplied with computers that are:

a) purchased from approved suppliers (eg those with a proven record of providing robust and resilient equipment)
b) tested prior to use
c) supported by maintenance arrangements
d) protected by physical controls (eg locks, alarms and indelible markings).

SM6.4.3

Computers used by staff working in remote locations should be supplied with:

a) standard, technical configurations (eg pre-configured to run a standard operating system, standard applications and common communications software)
b) a comprehensive set of system management tools (eg maintenance utilities and back-up software)
c) access control mechanisms to restrict access to the remote computer (eg using third party products)
d) up-to-date malware protection software, to protect against viruses, worms, trojan horses, spyware and adware
e) encryption software to protect information stored on the computer (eg using hard disk encryption) or transmitted by the computer (eg using a virtual private network (VPN) when connecting to the organisation's network).

SM6.4.4

Access to computers used in remote locations should be restricted by encrypting passwords and preventing logical access to the capabilities of unattended personal computers (eg by using password-protected screen savers or configuring computers with a terminal lock-out).

(continued on the next page)

Section SM6.4 Remote working (continued)

SM6.4.5

Staff that work in remote locations, including public areas (eg hotels, trains, airports and Internet cafes) or from home, should be:

a) authorised to work only in specified locations
b) equipped with the necessary skills to perform required security tasks (eg restricting access, taking back-ups and encrypting key files)
c) made aware of the additional risks associated with remote working (including the increased likelihood of theft of equipment or disclosure of confidential information)
d) provided with adequate technical support (eg via a helpdesk)
e) in compliance with legal and regulatory requirements (eg health and safety laws and data privacy regulations)
f) provided with alternative working arrangements in case of emergency.

SM6.4.6

Portable computers and devices should be protected against theft by:

a) providing users with physical locks or equivalent security devices
b) attaching identification labels
c) the use of indelible marking.

SM6.4.7

Additional controls should be implemented on workstations with the capability of connecting to the Internet, by:

a) using web browsers with a standard configuration
b) preventing users from disabling / modifying security options in web browsers
c) applying updates to web browser software quickly and efficiently
d) using software such as personal firewalls and malware protection
e) warning users of the dangers of downloading mobile code and the implications of accepting or rejecting 'cookies' (small text files containing information that can be used to identify a user returning to a website)
f) restricting the downloading of mobile code (eg by using firewalls) to block particular types of executables.

Section SM6.5 Third party access

Principle Connections from third parties (eg customers, clients and suppliers) should be uniquely identified, subjected to an information risk analysis, approved, and supported by contracts.

Objective To ensure that access to the organisation's information and systems is restricted to authorised third parties.

SM6.5.1

The provision of third party access should be supported by documented standards / procedures, which specify that, prior to connection:

a) the business risks associated with third party access are assessed
b) responsibility for authorising third party access is assigned to sufficiently senior staff
c) a due diligence exercise is performed and agreed security controls are implemented
d) testing is performed
e) agreed contracts are in place.

SM6.5.2

There should be methods in place to:

a) ensure that controls over third parties are commensurate with business risks
b) protect the interests of the organisation in relation to ownership of information and systems (eg retaining copyright of information, licensing software and maintaining ownership of physical resources supplied to third parties)
c) limit the liabilities of the organisation to third parties (eg through the use of contractual conditions and on-screen warnings)
d) comply with regulatory / statutory obligations (eg data privacy legislation)
e) make third parties accountable for their actions (eg by defining responsibilities, permissible actions and incident handling procedures in contracts).

SM6.5.3

When dealing with individual third party connections, there should be a process in place to:

a) achieve technical compatibility (eg using standards for information formats and communications protocols)
b) protect sensitive information stored on target systems or in transit to third party locations (eg using encryption)
c) log activity (eg to help track individual transactions and enforce accountability)
d) provide a single point of contact for dealing with problems (eg a helpdesk or call centre).

SM6.5.4

Access via individual third party connections should be managed by:

a) restricting methods of connection (eg to defined entry points and only through firewalls)
b) authenticating users in line with their job role
c) restricting the type of access granted (ie in terms of information, application capabilities and access privileges)
d) granting access to the organisation's information and systems on the principle of 'least access'
e) terminating connections when no longer required.

(continued on the next page)

Section SM6.5 Third party access (continued)

SM6.5.5

Connections that provide third party access should be individually identified, approved by the business owner, recorded (eg in an inventory or equivalent) and agreed by both parties in a documented contract.

SM6.5.6

Individuals responsible for managing third party connections should have access to:

a) information about the risks associated with third party access
b) standards / procedures outlining the steps to be taken to achieve secure connections
c) supporting tools (eg checklists, sample contracts and service level agreements)
d) sources of expertise they can turn to for specialist advice and assistance (eg the information security function).

Section SM6.6 Electronic commerce

Principle A process should be established to ensure that information security requirements are taken into account in electronic commerce initiatives across the organisation.

Objective To keep the increased risks associated with the development and deployment of electronic commerce within acceptable limits.

SM6.6.1

A top-level business manager (ie board level or equivalent) should be responsible for all electronic commerce initiatives.

SM6.6.2

A high-level committee or steering group should be established to co-ordinate electronic commerce initiatives, which includes representatives from key areas of the organisation involved in electronic commerce initiatives (eg top management, business owners, legal department, IT management, and the information security function).

SM6.6.3

The risks associated with electronic commerce initiatives should be subject to an information risk analysis (eg using the ISF's Information Risk Analysis Methodology (IRAM)).

SM6.6.4

There should be documented standards / procedures for managing enterprise-wide electronic commerce initiatives, which require that:

a) good information security practices are not sacrificed in the interest of speed of delivery
b) initiatives are driven by business requirements (ie they are not technology-led)
c) dependence on immature technology is minimised
d) the security implications of implementing vendor solutions are assessed.

SM6.6.5

A process should be established to ensure that key decision-makers:

a) understand the security requirements of customers
b) are aware of the full range of risks associated with electronic commerce and have not overlooked the main technical threats (eg lack of system capacity)
c) sign off residual risk
d) identify the security skills required to support electronic commerce initiatives and employ sufficient staff with the necessary skills (eg by using third party experts or training internal staff).

SM6.6.6

Prior to going live, electronic commerce initiatives should be tested rigorously (including volume testing involving very large numbers of users), reviewed by an information security specialist and signed off by top management.

(continued on the next page)

Section SM6.6 Electronic commerce (continued)

SM6.6.7

There should be a process to ensure that:

a) important domain name registrations are renewed (eg every two years)
b) domain names that could be used to masquerade as the organisation are registered by the organisation
c) websites are monitored that may have been set up using domain names similar to those used by the organisation (eg by using third party monitoring services)
d) illegitimate websites (eg those used for phishing attacks) are closed down as quickly as possible
e) relationships with internet service providers are covered by a service level agreement (SLA).

Section SM6.7 Outsourcing

Principle A process should be established to govern the selection and management of outsource providers, supported by documented agreements that specify the security requirements to be met.

Objective To ensure that security requirements are satisfied and maintained when the running of a particular environment or service is entrusted to an outsource provider.

SM6.7.1

A documented process should be established to govern the selection of outsource providers and the transfer of activity to them.

SM6.7.2

When determining the requirements for outsourcing, the organisation should:

a) evaluate information risks associated with outsourcing arrangements and the particular business functions that may be outsourced
b) identify particularly sensitive or critical environments
c) assess the information security practices and standards of potential outsource providers
d) consider interdependencies between the function to be outsourced and other business functions
e) develop exit strategies from the relationship in the eventuality of an early termination of the agreement (eg due to a dispute).

SM6.7.3

Before the management of a particular environment is transferred, information security controls should be agreed with the outsource provider and approvals for the transfer obtained from relevant business owners.

SM6.7.4

Documented agreements (eg contracts) should be established that require outsource providers to:

a) comply with good practice for information security
b) provide information about information security incidents
c) maintain the confidentiality of information gained through the outsourcing agreement
d) protect the integrity of information used in the course of work (ie to ensure it is complete, accurate and valid)
e) ensure the availability of information and systems (eg by providing resilient equipment and guaranteeing response times).

SM6.7.5

Agreements should require that outsource providers:

a) limit access to the assets of the organisation to authorised staff
b) protect personally identifiable information
c) provide business continuity arrangements
d) meet legal and regulatory requirements (eg data protection legislation as part of the Payment Card Industry (PCI) Data Security Standard)
e) assure the quality and accuracy of work performed
f) return or destroy information, software or equipment on an agreed date, or upon request
g) define the way in which the outsource provider is permitted to further outsource to other third parties
h) follow a change management process
i) provide effective information security incident management.

(continued on the next page)

Section SM6.7 Outsourcing (continued)

SM6.7.6

A process should be agreed to deal with security issues via an agreed point of contact(s) within the outsource provider.

SM6.7.7

Agreements should specify: the right to audit the outsource provider's activities; details of licensing arrangements; and the ownership of intellectual property rights and information.

SM6.7.8

Contingency arrangements for the organisation should be established to manage outsourced environments in the event that the outsource provider becomes unavailable (eg due to a disaster or dispute).

Section SM6.8 Instant messaging

Principle Instant messaging services should be protected by setting management policy, deploying instant messaging application controls and correctly configuring the security elements of an instant messaging infrastructure.

Objective To ensure that instant messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

SM6.8.1

There should be documented standards / procedures for instant messaging services (ie the application and supporting infrastructure) which include:

a) guidelines for business and personal use (eg prohibition of personal use)
b) the types of instant messaging services permitted (eg public services such as AOL, Google Talk, Windows Messenger and Yahoo!, or internal services such as Lotus Sametime, Windows Meeting Space, Webex and Jabber)
c) user guidelines for acceptable use (eg prohibition of offensive statements)
d) details of any monitoring activities to be performed.

SM6.8.2

The security of instant messaging applications should be improved by:

a) disabling inappropriate features (eg file sharing, video and audio)
b) using encryption to protect the contents of sensitive messages
c) enabling malware checking at the desktop (eg to compensate for port agile instant messaging software that might bypass malware checking at messaging gateways)
d) logging key events (eg to maintain records for regulatory purposes)
e) directing instant messaging traffic through a content filter.

SM6.8.3

Protection of the instant messaging infrastructure should be improved by:

a) employing a standard client configuration for the instant messaging application
b) 'hardening' instant messaging servers (eg by locking down the operating system and application)
c) configuring firewalls to block unauthorised instant messaging traffic (eg by blocking known instant messaging ports).

Area SM7

MANAGEMENT REVIEW

An accurate understanding of the information security condition of the organisation is required in order to manage information security effectively. Accordingly, this area covers the arrangements needed to provide decision-makers with sound information on the security condition of information and systems throughout the organisation.

Section SM7.1 Security audit / review

Principle The information security status of critical IT environments should be subject to thorough, independent and regular security audits / reviews.

Objective To provide individuals who are responsible for particular IT environments, and top management, with an independent assessment of the information security condition of those environments.

SM7.1.1

Independent security audits / reviews should be performed regularly for environments that are critical to the success of the organisation, including:

a) business applications
b) computer installations and networks
c) systems development activities
d) key enterprise-wide security activities (eg managing a security architecture, running awareness programmes or monitoring information security arrangements)
e) end user environments (eg a claims processing department, sales and marketing office, research and development operation, manufacturing plant or call centre).

SM7.1.2

Security audits / reviews should be:

a) agreed with the owner of the environments under review
b) performed by individuals who are equipped with sufficient technical skills and knowledge of information security
c) conducted thoroughly (in terms of scope and extent) to provide assurance that security controls function as required
d) focused on ensuring that controls are effective enough to reduce risk to an acceptable level
e) supplemented by the use of automated software tools
f) validated by competent individuals
g) complemented by reviews carried out by independent third parties.

(continued on the next page)

Section SM7.1 Security audit / review (continued)

SM7.1.3

Security audit / review activity should be managed by:

a) agreeing requirements for special processing routines or tests (eg penetration testing) with the owners of the environments under review
b) restricting access to systems by audit / review teams
c) monitoring and logging the activities of audit / review teams
d) disposing of business information copied for the purpose of audits / reviews as soon as it is no longer required
e) protecting software tools used in carrying out audits / reviews (eg by keeping them separate from tools / utilities used in the live environment, and holding them in secure storage facilities, such as restricted software libraries).

SM7.1.4

Recommendations following security audits / reviews should be agreed with the owners of environments under review and reported to top management.

Section SM7.2 Security monitoring

Principle The information security condition of the organisation should be monitored regularly and reported to top management.

Objective To provide top management with an accurate, comprehensive and coherent assessment of the security condition of the organisation.

SM7.2.1

There should be arrangements for monitoring the information security condition of the organisation, which are documented, agreed with top management (eg board-level executives or equivalent) and performed regularly.

SM7.2.2

Analysis performed as part of security monitoring arrangements should be:

a) based on quantitative security metrics (eg the number, frequency and business impact of information security incidents; internal and external audit findings; operational security statistics, such as firewall log data, patch management details and number of spam e-mails; and costs associated with financial losses, legal or regulatory penalties and fraud)
b) presented in a standard format (eg security dashboards, cockpits or balanced scorecards).

SM7.2.3

Information collected as part of security monitoring arrangements should include details about all aspects of information risk (eg criticality of information, identified vulnerabilities and level of threats, potential business impacts and status of security controls in place).

SM7.2.4

Information about the security condition of the organisation should be provided to key decision-makers (including top management, members of a high-level security committee, and relevant external bodies).

SM7.2.5

Security monitoring arrangements should provide key decision-makers with an informed view of:

a) the effectiveness and efficiency of information security arrangements
b) areas where improvement is required
c) information and systems that are subject to an unacceptable level of risk
d) performance against quantitative, objective targets
e) actions required to help minimise risk (eg reviewing the organisation's risk appetite; understanding the information security threat environment; and encouraging business and system owners to remedy unacceptable risks).

SM7.2.6

Security monitoring arrangements should provide key decision-makers with financial information including the:

a) cost of security controls (eg acquisition and upgrade of security products and services, implementation costs, operational and maintenance costs, and the cost of staff)
b) financial impact of information security incidents (eg loss of sales; cost of delayed deliveries; fraud; and cost of recovery, including staff time, hardware, software and services)
c) return on security investment (ROSI) of deployed controls (eg the non-financial benefits, financial benefits and costs).

(continued on the next page)

Section SM7.2 Security monitoring (continued)

SM7.2.7

Security monitoring arrangements should enable key decision-makers to:

a) manage information risk effectively
b) relate information risk to operational / business risk.
c) demonstrate compliance with legal and regulatory requirements, and internal information security standards / procedures.

SM7.2.8

Information generated by monitoring the information security condition of the organisation should be used to measure the effectiveness of the information security strategy, information security policy and security architecture.

Critical Business Applications

A critical business application requires a more stringent set of security controls than other applications. By understanding the business impact of a loss of confidentiality, integrity or availability of information, it is possible to establish the level of importance of an application. This provides a sound basis for identifying information risks and determining the level of protection required to keep information risks within acceptable limits.

Critical Business Applications

CB1 Business requirements for security

CB1.1 Confidentiality requirements

CB1.2 Integrity requirements

CB1.3 Availability requirements

CB2 Application Management

CB2.1 Roles and responsibilities

CB2.2 Application controls

CB2.3 Change management

CB2.4 Information security incident management

CB2.5 Business continuity

CB2.6 Sensitive information

CB3 User Environment

CB3.1 Access control

CB3.2 Application sign-on process

CB3.3 Workstation protection

CB3.4 Security awareness

CB4 System Management

CB4.1 Service agreements

CB4.2 Resilience

CB4.3 External connections

CB4.4 Back-up

CB5 Local Security Management

CB5.1 Local security co-ordination

CB5.2 Information classification

CB5.3 Information risk analysis

CB5.4 Security audit / review

CB6 Special Topics

CB6.1 Third party agreements

CB6.2 Cryptographic key management

CB6.3 Public key infrastructure

CB6.4 Web-enabled applications

Area CB1
BUSINESS REQUIREMENTS FOR SECURITY

Business applications vary enormously in their importance to the business; hence the level of protection required also varies. Accordingly, this area identifies the information security requirements of the application.

Section CB1.1 Confidentiality requirements

Principle The business impact of unauthorised disclosure of information associated with the application should be assessed.

Objective To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the application.

CB1.1.1

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have a financial impact on the organisation in terms of:

a) loss of sales, orders or contracts
b) loss of tangible assets
c) penalties / legal liabilities
d) unforeseen costs
e) depressed share price.

CB1.1.2

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have an operational impact on the organisation in terms of:

a) loss of management control
b) loss of competitiveness
c) new ventures held up
d) breach of operating standards.

CB1.1.3

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have a customer-related impact on the organisation in terms of:

a) delayed deliveries to customers or clients
b) loss of customers or clients
c) loss of confidence by key institutions
d) damage to reputation.

CB1.1.4

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have an employee-related impact on the organisation in terms of:

a) reduction in staff morale / productivity
b) injury or death.

Section CB1.2 Integrity requirements

Principle The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the application should be assessed.

Objective To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the application.

CB1.2.1

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have a financial impact on the organisation in terms of:

a) loss of sales, orders or contracts
b) loss of tangible assets
c) penalties / legal liabilities
d) unforeseen costs
e) depressed share price.

CB1.2.2

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have an operational impact on the organisation in terms of:

a) loss of management control
b) loss of competitiveness
c) new ventures held up
d) breach of operating standards.

CB1.2.3

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have a customer-related impact on the organisation in terms of:

a) delayed deliveries to customers or clients
b) loss of customers or clients
c) loss of confidence by key institutions
d) damage to reputation.

CB1.2.4

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have an employee-related impact on the organisation in terms of:

a) reduction in staff morale / productivity
b) injury or death.

Section CB1.3 Availability requirements

Principle The business impact of business information stored in or processed by the application being unavailable for any length of time should be assessed.

Objective To document and agree the availability requirements (the need for information to be accessible when required) of the application.

CB1.3.1

The analysis of availability requirements should determine how a loss of availability of information could have a financial impact on the organisation in terms of:

a) loss of sales, orders or contracts
b) loss of tangible assets
c) penalties / legal liabilities
d) unforeseen costs
e) depressed share price.

CB1.3.2

The analysis of availability requirements should determine how a loss of availability of information could have an operational impact on the organisation in terms of:

a) loss of management control
b) loss of competitiveness
c) new ventures held up
d) breach of operating standards.

CB1.3.3

The analysis of availability requirements should determine how a loss of availability of information could have a customer-related impact on the organisation in terms of:

a) delayed deliveries to customers or clients
b) loss of customers or clients
c) loss of confidence by key institutions
d) damage to reputation.

CB1.3.4

The analysis of availability requirements should determine how a loss of availability of information could have an employee-related impact on the organisation in terms of:

a) reduction in staff morale / productivity
b) injury or death.

CB1.3.5

Business requirements should take into account the critical timescale of the application (ie the timescale beyond which an outage is unacceptable to the organisation).

Area CB2
APPLICATION MANAGEMENT

Keeping business risks within acceptable limits requires a coherent set of information security arrangements. Accordingly, this area covers the roles and responsibilities required (including business ownership), integral application controls and additional controls needed for handling or transferring sensitive information. In addition, this area covers general management controls including change management, information security incident management and business continuity.

Section CB2.1 Roles and responsibilities

Principle An owner should be identified for the application, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To assign ownership of the application, achieve individual accountability, provide a sound management structure for staff running or using it and give responsible individuals a vested interest in its protection.

CB2.1.1

An owner should be appointed to be in charge of the application. Responsibilities of the application owner should be assigned to a business manager, who should accept the responsibilities (including those for information security) associated with this role.

CB2.1.2

There should be documented standards / procedures for administering the application, which are approved by the application owner and kept up-to-date.

CB2.1.3

Standards / procedures should specify methods of:

a) administering users (eg adding new business users, updating access privileges, and revoking user access rights)
b) updating key 'static' business information (eg customer master files, currency exchange rates or product details)
c) monitoring key security-related events (eg system crashes, unsuccessful log-in of authorised users, and unsuccessful changes to access privileges)
d) validating processes / data
e) reviewing error / exception reports
f) identifying potential security weaknesses / breaches (eg as a result of analysing user behaviour or patterns of network traffic).

CB2.1.4

Individuals involved in administering the application should be:

a) assigned clear responsibilities
b) able to administer the application correctly
c) competent to deal with error, exception and emergency conditions
d) aware of information security principles and associated good practice
e) sufficient in number to handle required workloads at all times.

(continued on the next page)

Section CB2.1 Roles and responsibilities (continued)

CB2.1.5

Individuals involved in administering the application should be organised to minimise:

a) reliance on key individuals (eg by arranging alternative cover or appointing deputies)
b) the risk of theft, fraud, error and unauthorised changes to information (eg by supervision of activities, prohibition of lone working and segregation of duties).

Section CB2.2 Application controls

Principle The full range of application controls should be considered, and required controls identified.

Objective To build in the required application controls to protect information stored in or processed by the application.

CB2.2.1

Information entered into the application (ie data entry) should be checked to ensure its validity (eg by using range, consistency and 'hash total' checks) and completeness (eg comparison with control balances or original documentation).

CB2.2.2

Arrangements should be made to ensure that:

a) information cannot be overwritten accidentally (eg by write-protecting key fields or files)
b) the processing of information is validated (eg by record counts, and hash, session, batch or balancing totals)
c) changes to key files and parameters are reviewed (eg by inspecting the contents of records before and after they have been changed)
d) unauthorised or incorrect changes to information are detected (eg by inspecting change logs, using automated 'checksum' tools or reconciling data back to its original source).

CB2.2.3

The integrity (completeness, accuracy and validity) of information processed by the application should be confirmed by checking against external sources (eg by comparing against order processing logs, customer / supplier records, or physical stock).

CB2.2.4

Application output should be checked to ensure its validity (eg by reconciling control counts to physical records to ensure all data is processed or performing plausibility checks to ensure output is reasonable).

CB2.2.5

The application should be protected by:

a) building error and exception reports into the application
b) preventing information about the internal workings of the application (eg in application responses or error messages) from being disclosed
c) minimising manual intervention (eg by automating processes).

CB2.2.6

Host systems (eg servers running operating systems such as UNIX, Linux or Windows) that support applications, should be configured to:

a) restrict non-essential or redundant services (eg X Windows, Open Windows, web browsers, Telnet and FTP)
b) disable unnecessary or insecure user accounts (eg the 'Guest' account (or equivalent) for Windows XP and UNIX systems)
c) change important security-related parameters (eg passwords) to be different from the default values set by suppliers
d) provide a reliable event log (eg system crashes, unsuccessful log-in of authorised users, and unsuccessful changes to access privileges).

CB2.2.7

Event logs of the application should be reviewed regularly (eg by using automated tools).

Section CB2.3 Change management

Principle Changes to the application should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise the security of the application.

CB2.3.1

A change management process should be established, which covers all types of change (eg upgrades and modifications to application and software, modifications to business information, emergency 'fixes', and changes to the computers / networks that support the application).

CB2.3.2

The change management process should be documented, and include:

a) approving and testing changes to ensure that they do not compromise security controls
b) performing changes and signing them off to ensure they are made correctly and securely
c) reviewing completed changes to ensure that no unauthorised changes have been made.

CB2.3.3

Prior to changes being applied to the live environment:

a) change requests should be documented (eg on a change request form) and accepted only from authorised individuals
b) changes should be approved by an appropriate business representative
c) the potential business impacts of changes should be assessed (eg in terms of the overall risk and impact on other components of the application)
d) changes should be tested to help determine the expected results (eg of deploying the patch into the live environment)
e) changes should be reviewed to ensure that they do not compromise security controls (eg by checking software to ensure it does not contain malicious code, such as a trojan horse or a virus)
f) back-out positions should be established so that the application can recover from failed changes or unexpected results.

CB2.3.4

Changes to the application should be:

a) performed by skilled and competent individuals who are capable of making changes correctly and securely
b) supervised by an IT specialist
c) signed off by an appropriate business representative.

(continued on the next page)

Section CB2.3 Change management (continued)

CB2.3.5

Arrangements should be made to ensure that once changes have been applied:

a) version control is maintained (eg using configuration management)
b) a record is maintained, showing what was changed, when, and by whom (eg using automated helpdesk / service desk software)
c) details of changes are communicated to relevant individuals (eg associated users, business managers and relevant third parties)
d) checks are performed to confirm that only intended changes have been made (eg by comparing code against a control version or checking 'before and after' contents of key records, such as within customer master files)
e) documents associated with the application are updated (eg design information, system configuration, implementation details, and records of all changes to the application)
f) the classification of information associated with the application is reviewed.

CB2.3.6

Checks should be performed on a regular basis to confirm that only intended changes have been made (eg by using code comparison programs or checking 'before and after' contents of key records such as customer master files).

Section CB2.4 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

CB2.4.1

There should be a documented information security incident management process that applies to the application.

CB2.4.2

The information security incident management process should include:

a) identifying information security incidents
b) responding to information security incidents
c) recovering from information security incidents
d) following up information security incidents.

CB2.4.3

Information security incidents should be:

a) reported to a predetermined contact (eg a helpdesk, telephone hot line or specialist IT team / department)
b) recorded in a log, or equivalent (eg using an automated information security incident management system)
c) categorised and classified (eg according to their severity and type).

CB2.4.4

The business impact of serious information security incidents should be assessed by an application specialist, the application owner and an information security specialist.

CB2.4.5

The response to information security incidents should include:

a) analysing available information (eg application and system event logs)
b) handling necessary evidence (eg labelling it and storing it in a safe location to prevent unauthorised tampering)
c) investigating the cause of information security incidents (eg with assistance from the information security incident management team)
d) containing and eradicating the information security incident (eg by making changes to access control or terminating network connections).

CB2.4.6

The recovery of information security incidents should involve:

a) rebuilding applications (and supporting IT facilities) to a previously known secure state (ie the same state they were in before the information security incident occurred)
b) restoring from information that has not been compromised by the information security incident
c) closure of the information security incident.

(continued on the next page)

Section CB2.4 Information security incident management (continued)

CB2.4.7

Following recovery from information security incidents:

a) reviews should be performed to determine the cause (eg by performing a root cause analysis) and effect of the information security incident and corresponding recovery actions
b) forensic investigations should be performed if required (eg for legal purposes or serious information security incidents, such as fraud)
c) existing security controls should be examined to determine their adequacy
d) corrective actions should be undertaken to minimise the risk of similar incidents occurring
e) details of the information security incident should be documented in a post-incident report.

Section CB2.5 Business continuity

Principle A business continuity plan should be established, supported by contingency arrangements, and tested regularly.

Objective To enable the business processes associated with the application to continue in the event of a disaster.

CB2.5.1

Business continuity should be the responsibility of a specific individual or working group.

CB2.5.2

The application should be supported by a documented business continuity plan, based on the results of a documented risk analysis, reviewed by key staff (eg information security specialists and user representatives), and signed off by an appropriate business representative.

CB2.5.3

The business continuity plan should specify:

a) recovery tasks to be carried out, in priority order
b) responsibilities of individuals, with nominated deputies
c) arrangements for the safe storage of plans, and their retrieval in case of emergency
d) testing of information security arrangements (eg rebuild and configuration of firewalls, malware protection software and intrusion detection mechanisms).

CB2.5.4

Relevant staff should be made aware of the responsibilities assigned to them in the business continuity plan.

CB2.5.5

The application should be supported by business continuity arrangements (eg a separate processing facility ready for immediate use or a contract with a specialist business continuity arrangements provider) in case of a disaster or emergency.

CB2.5.6

Business continuity arrangements should cover the prolonged unavailability of:

a) system or application software
b) critical information (eg business information, documentation, back-up files)
c) computer or network equipment, cabling or links
d) key staff (eg information security specialists, IT or user representatives)
e) buildings, machine rooms, power, communications and other vital services
f) access to systems or buildings (eg due to police, military or terrorist action, natural disaster, or withdrawal of transport services).

CB2.5.7

Steps should be taken to ensure business continuity arrangements will work within critical timescales by carrying out:

a) tests of alternative processing arrangements (eg running the application from a back-up site)
b) realistic simulations, involving both users and IT staff
c) tests of information security arrangements (eg rebuild and configuration of firewalls, malware protection software and intrusion detection mechanisms).

Section CB2.6 Sensitive information

Principle Additional protection should be provided for applications that involve handling sensitive material or transferring sensitive information.

Objective To preserve the integrity of sensitive information and protect it from unauthorised disclosure.

CB2.6.1

The transfer of sensitive information (eg involving other business applications or third parties) should involve the use of cryptography to:

a) protect the confidentiality of sensitive information when transferred
b) determine if critical information has been altered during transfer
c) enable the identity of the originator of critical information to be proven (eg using digital signatures to provide non-repudiation).

CB2.6.2

Sensitive physical material associated with the application (eg smartcards, access tokens, blank cheques, print-outs of personal information and removable storage media containing PIN data) should be:

a) stored in a physically secure location (eg in a fireproof safe and according to the manufacturer's specifications)
b) protected in transit (eg by recording authorised recipients, clearly marking all material and confirming receipt)
c) monitored by recording its issue and use
d) disposed of in a secure manner when no longer required (eg by using methods such as erasure, incineration or shredding)
e) protected from loss, theft and unauthorised disclosure (eg by immediate removal from printers, facsimile machines or photocopiers).

Area CB3
USER ENVIRONMENT

Critical business applications can be used by internal or external business or technical users. These individuals may be sited locally or at a remote location, often with differing business and security requirements. Accordingly, this area covers the disciplines required to control access to the application, configure workstations and ensure that users are aware of information security and understand their personal responsibilities.

Section CB3.1 Access control

Principle Access to the application and associated information should be restricted to authorised individuals.

Objective To ensure that only authorised individuals are granted access to the application, and that individual accountability is assured.

CB3.1.1

Users of the application should be:

a) identified (eg by a unique UserID)
b) authenticated (eg by a password or token)
c) provided with the minimum functionality required to perform their role.

CB3.1.2

System administrators and users of critical business applications should be subject to strong authentication mechanisms (eg using smartcards, biometrics or tokens).

CB3.1.3

There should be a method of ensuring that users do not share identification or authentication details.

CB3.1.4

There should be a process for issuing new or changed passwords that:

a) ensures that disclosure of passwords are minimised when they are communicated to the user (eg using encrypted e-mails or forcing the user to change passwords when they first use them)
b) involves the target user directly (ie the person to whom the password uniquely applies)
c) verifies the identity of the target user (eg via a special code or through independent confirmation)
d) ensures that passwords are changed regularly.

CB3.1.5

Users' access rights should be:

a) restricted according to a defined policy (eg on a 'need to know' or 'need to restrict' basis)
b) restricted according to users' individual roles
c) authorised by the application owner
d) revoked promptly when an individual user is no longer entitled to them
e) enforced by automated access control mechanisms to ensure individual accountability.

(continued on the next page)

Section CB3.1 Access control (continued)

CB3.1.6

User access to the application should be logged (eg in an event log). Event logs should be configured to:

a) record appropriate event types (eg system crash, object deletion and failed password)
b) incorporate relevant event attributes in event entries (eg IP address, user identity, time and date, protocol and port used, files or system utilities accessed, method of connection, name of device and object name).

CB3.1.7

Event logs should be:

a) reviewed regularly (eg to help identify suspicious or unauthorised activity)
b) retained for a defined period (eg to comply with legal and regulatory requirements)
c) protected against unauthorised change.

CB3.1.8

Vendor-supplied authentication details for high-level privilege accounts (eg those used to perform application administration) should be changed before applications are used.

Section CB3.2 Application sign-on process

Principle Users should be subject to a rigorous sign-on process before being provided with access to the application.

Objective To ensure that only authorised users can gain access to the application.

CB3.2.1

There should be a sign-on process that users must follow before they are provided with access to the application, which should enable individual users to be identified (eg using unique UserIDs).

CB3.2.2

Sign-on mechanisms should be configured so that they:

a) validate sign-on information only when it has all been entered
b) limit the number of unsuccessful sign-on attempts which are permitted (eg a re-try limit of three)
c) restrict additional sign-on attempts
d) limit the duration of any one sign-on session
e) are re-enabled automatically after interruption (eg following a disconnection from the application).

CB3.2.3

Sign-on mechanisms should be configured to provide information so that they:

a) display no identifying details until after sign-on is completed successfully
b) warn that only authorised users are permitted access
c) record all successful and unsuccessful sign-on attempts
d) advise users (on successful sign-on) of the date / time of their last successful sign-on and all unsuccessful sign-on attempts since their most recent successful sign-on.

CB3.2.4

Sign-on mechanisms should be configured so that they do not store authentication details as clear text in automated routines (eg in scripts, macros or cache memory).

CB3.2.5

The approval of an appropriate business representative should be obtained before any important features of the sign-on process are bypassed, disabled or changed.

Section CB3.3 Workstation protection

Principle Workstations connected to the application should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements, and protected by physical controls.

Objective To ensure workstations operate as intended, are available when required and do not compromise the security of the application.

CB3.3.1

Workstations (ie desktop computers and laptop computers) connected to critical business applications should be supported by documented standards / procedures, which cover:

a) implementation and maintenance of workstations
b) provision of software to protect workstations (eg system management tools, access control mechanisms, malware protection software and encryption capabilities)
c) software configuration of workstations (eg employing standard builds and relevant web browser settings)
d) protection against malicious mobile code (eg executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that have been written deliberately to perform unauthorised functions).

CB3.3.2

Workstations should be:

a) purchased from approved suppliers (ie those with a proven record of providing robust and resilient equipment)
b) tested prior to use
c) supported by maintenance arrangements
d) protected by physical and environmental controls
e) provided with standard technical configurations (eg running a standard operating system, standard applications and common communications software).

CB3.3.3

Workstations should be protected by the use of:

a) a comprehensive set of system management tools (eg maintenance utilities, remote support, enterprise management tools and back-up software)
b) access control mechanisms (ie to restrict access to the workstation)
c) up-to-date malware protection software, to protect against malicious software (eg computer viruses, worms, trojan horses, spyware, adware and malicious mobile code)
d) encryption software to safeguard information stored on internal and external hard disk drives
e) automatic time-out after a set period of activity
f) restrictions on the use of removable storage media (eg prohibition of personal use of external hard disk drives and USB memory sticks).

Malware typically includes computer viruses, worms, trojan horses, spyware, adware and malicious mobile code (executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions).

CB3.3.4

Portable devices (eg laptop computers and Personal Digital Assistants (PDAs)) should be protected against theft by:

a) providing users with physical locks or equivalent security devices
b) attaching identification labels
c) the use of indelible marking.

(continued on the next page)

Section CB3.3 Workstation protection (continued)

CB3.3.5

Workstations that can connect to the Internet should be protected by:

a) using web browsers with a standard, secure configuration
b) preventing users from disabling security options in web browsers
c) applying updates to web browser software quickly and efficiently
d) using personal firewalls
e) warning users of the dangers of downloading mobile code and the implications of accepting or rejecting 'cookies' (small text files containing information that can be used to identify a user returning to a website)
f) restricting the downloading of mobile code (eg executable code such as Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions).

Section CB3.4 Security awareness

Principle Users of the application should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure users of the application apply security controls and prevent important information used in the application from being compromised or disclosed to unauthorised individuals.

CB3.4.1

Users of the application should be covered by an information security policy. Users should be aware of, and comply with, the information security policy.

CB3.4.2

Users of the application should:

a) take part in a security awareness programme (eg attend structured awareness training seminars)
b) be provided with information security education / training (eg using techniques such as presentations and computer-based training (CBT))
c) be supplied with specialised security awareness material (eg brochures, reference cards, posters and electronic documents delivered via an organisation's intranet).

Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities.

CB3.4.3

Users of the application should be made aware of:

a) the meaning of information security (ie the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the application
c) the importance of complying with information security policies and applying associated standards / procedures
d) their personal responsibilities for information security.

CB3.4.4

Users of the application should be made aware that they are prohibited from:

a) unauthorised use of information or systems
b) using the application for purposes that are not work-related
c) making sexual, racist or other statements that may be offensive (eg when using e-mail, instant messaging, the Internet, or the telephone)
d) making obscene, discriminatory or harassing statements, which may be illegal (eg when using e-mail, instant messaging, the Internet, or the telephone)
e) downloading illegal material (eg with obscene or discriminatory content)
f) using unauthorised information facilities or equipment (eg unauthorised third party software, USB sticks or modems)
g) unauthorised copying of information or software
h) disclosing confidential information (eg customer records, product designs and pricing policies) to unauthorised individuals
i) compromising passwords (eg by writing them down or disclosing them to others)
j) using personally identifiable information (ie information that can be used to identify an individual person) unless explicitly authorised
k) tampering with evidence in the case of information security incidents that may require forensic investigation.

(continued on the next page)

Section CB3.4 Security awareness (continued)

CB3.4.5

Users of the application should be warned of the dangers of being overheard when discussing business information over the telephone or in public places (eg train carriages, airport lounges or bars).

Area CB4
SYSTEM MANAGEMENT

To enable applications to function, they have to run on one or more computers and typically make use of one or more networks. Accordingly, this area covers service agreements, the resilience of the application, external connections and the back-up of essential information and software.

Section CB4.1 Service agreements

Principle Computer and network services required to support the application should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.

Objective To define the business requirements for providers of any computer or network services that support the application, including those for information security, and to ensure they are met.

CB4.1.1

The computer and network services required to support an application should be defined in documented service agreements (eg contracts or service level agreements).

A service level agreement (SLA) should include all key elements, such as: who is in charge of the application (ie the application owner); who is in charge of delivering the required service (eg an internal or external service provider); capacity requirements; maximum permissible down-time; and criteria for measuring the level of service.

CB4.1.2

Service agreements should specify:

a) who is in charge of the application (ie the application owner)
b) who is in charge of delivering the required service (eg an internal specialised department or external service provider, such as an ISP)
c) the capacity requirements of the application (eg the projected number of users, normal and peak volumes of work to be handled, response times and transmission rates)
d) maximum permissible down-time.

CB4.1.3

Service agreements should specify requirements for:

a) access restrictions (eg restricting business users and support staff; permissible / disallowed methods of connection; and access points)
b) authentication methods
c) arrangements for ensuring business and system continuity of service
d) change management
e) information security incident management
f) segregation of duties and facilities.

CB4.1.4

Service agreements should be signed off by an appropriate business representative (eg the individual in charge of a business process or activity) and the service provider.

(continued on the next page)

Section CB4.1 Service agreements (continued)

CB4.1.5

Service arrangements should be made with the service provider to deal with security issues via a single point of contact and through an individual who is sufficiently senior and competent to deal with security issues effectively.

CB4.1.6

Service arrangements should be made to:

a) restrict the use of services to those provided by reputable parties
b) obtain independent confirmation of the security controls applied by the service provider.

CB4.1.7

The conditions of service agreements should be enforced, and the achievement of service targets reviewed regularly.

Section CB4.2 Resilience

Principle The application should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective To ensure that the application is available when required.

CB4.2.1

The application should be supported by up-to-date makes / models of software and hardware (ie rather than by obsolete and unsupported products) that can handle peak workloads.

CB4.2.2

Components that support the application (eg software, documentation, supporting computers / networks) should be identified and recorded in an inventory, or equivalent.

CB4.2.3

The resilience of the application should be improved by:

a) duplicating computer hardware components (eg processors, hard disk drives, network interface cards and memory) to create fault-tolerant systems
b) processing information simultaneously at multiple locations (eg using hot stand-by)
c) automatically identifying and recovering transactions following a system failure
d) using resilient data storage (eg disk mirroring and RAID technology)
e) running the application on a dedicated computer, mainframe partition or virtual server (ie a partition on a server running virtualisation software)
f) supporting the application through a dedicated network or sub-network
g) preventing the transfer of information from any connected systems that do not have acceptable security controls (eg using firewalls).

CB4.2.4

Critical computer and network equipment that support the application should be protected by uninterruptible power supplies (UPS).

CB4.2.5

An alternative source of power (eg a back-up electricity generator) should be provided to enable the application, and supporting systems, to continue running in the event of an extended power failure to the site (ie the premises where IT facilities are located).

Section CB4.3 External connections

Principle All external connections to the application should be individually identified, verified, recorded, and approved.

Objective To ensure that only authorised individuals are granted access to the application via external connections.

CB4.3.1

External connections to the application (eg those used by staff working in remote locations or by authorised third parties) should be identified individually, and signed off by an appropriate business representative (eg the individual in charge of a business process or activity).

CB4.3.2

A record of external connections should be maintained (eg in an inventory or equivalent, such as a database).

CB4.3.3

External access to the application should be subject to strong authentication (eg challenge / response devices featuring one-time passwords, smartcards, tokens or biometrics).

CB4.3.4

External access to the application should be restricted by:

a) routing application-related traffic through firewalls (eg stateful inspection firewalls (typically located in the perimeter of a network), application proxy firewalls (typically located between internal networks) and application firewalls (typically located close to the application))
b) limiting the methods of connection (eg via broadband, ISDN or dial-up)
c) granting access only to specified parts of the application.

CB4.3.5

External access should be prevented when no longer required by removing or disabling:

a) network connections (eg by physically removing a network connection, modifying firewall rules, updating access control lists and configuring routing tables on network routers)
b) key components (eg redundant modems, communications lines and software configuration settings).

Section CB4.4 Back-up

Principle Back-ups of essential information and software used by the application should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential information or software required by the application can be restored within critical timescales.

CB4.4.1

Back-ups of essential information and software (eg business information, systems information and application information) should be performed frequently enough to meet business requirements.

CB4.4.2

Back-ups should be:

a) performed using a back-up management package to strengthen the security of backed-up information
b) encrypted to protect important information (eg in the event back-up media is stolen or is lost in transit to an alternative location, such as an off-site storage facility)
c) recorded in a log (or equivalent), which includes details about backed-up data, the date and time of the back-up, and the back-up media used
d) verified to ensure that backed-up software and information can be restored successfully.

CB4.4.3

Back-up arrangements should enable software and information to be restored within a critical timescale (ie the timescale beyond which an outage is unacceptable to the organisation).

CB4.4.4

Back-ups should be protected from loss, damage and unauthorised access, by:

a) storing them in a computer media fireproof safe on-site, to enable important information to be restored quickly
b) keeping copies off-site, to enable the application to be restored using alternative facilities in the event of a disaster
c) restricting access to authorised staff (eg through the use of access control software, physical locks and keys).

Area CB5
LOCAL SECURITY MANAGEMENT

The security controls applied to a business application should be proportional to business risk. Accordingly, this area covers the arrangements made to identify the importance of information stored in or processed by the application, the associated business risks and the level of protection required. It also addresses local security co-ordination and the need for the application to be subject to thorough, independent and regular security audits / reviews.

Section CB5.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate information security activities associated with the application.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

CB5.1.1

The application owner should have overall responsibility for information security in relation to the application. A local information security co-ordinator should be appointed to be responsible for co-ordinating the information security arrangements of the application and acting as a single point of contact on information security issues.

CB5.1.2

Local information security co-ordinator(s) should have:

a) a sound understanding of their information security roles and responsibilities
b) sufficient technical skills, time, tools (eg checklists and specialist software products) and authority to carry out their assigned roles
c) access to in-house or external expertise in information security
d) documented standards / procedures to support day-to-day security activities
e) up-to-date information related to information security issues (eg users' security requirements, emerging threats and newly discovered vulnerabilities) and techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture)
f) a channel of communication with the information security function.

CB5.1.3

The local information security co-ordinator(s) should meet regularly with the application owner to review the status of information security in the application and agree information security activities to be performed.

Section CB5.2 Information classification

Principle Information stored in or processed by critical business applications should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to the application, thereby preventing unauthorised disclosure.

CB5.2.1

Information associated with the application should be subject to an information classification scheme (ie a method of classifying information according to its level of confidentiality), which complies with enterprise-wide standards / procedures for information classification.

Some organisations also take into account requirements for integrity (ie the need for information to be valid, accurate and complete) and availability (ie the need for information to be accessible when required) when classifying information.

CB5.2.2

The information classification scheme should:

a) take account of the potential business impact from the loss of confidentiality of information
b) be used to determine varying levels of confidentiality of information (eg top secret, company-in-confidence and public).

CB5.2.3

The information classification scheme should be used to classify:

a) information stored in paper form (eg contracts, plans and system documentation held in hard copy form)
b) information held in electronic form (eg business transactions, financial statistics, product design details and customer files).

Information classification typically involves labelling of:

- information stored in paper form (eg using rubber ink stamps, adhesive labels, hologram lamination)
- information stored in electronic form (eg using electronic watermarking, labelling headers and footers, using filename conventions)
- electronic communications (eg using digital signatures and including the classification in the subject header of e-mails).

CB5.2.4

Information classifications associated with the application should be:

a) signed off by the relevant business owner
b) reviewed regularly and when changes are made to the application.

CB5.2.5

Information classification details associated with the application should be recorded in:

a) an inventory, or equivalent (eg a database, specialised piece of software, or on paper)
b) agreements with service providers.

(continued on the next page)

Section CB5.2 Information classification (continued)

CB5.2.6

Information classification details should include:

a) the classification of the information (eg top secret, company-in-confidence and public)
b) the identity of the information owner
c) a brief description of the information classified.

Section CB5.3 Information risk analysis

Principle The application should be subject to an information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed.

Objective To identify key information risks associated with the application, and determine the security controls required in order to keep those risks within acceptable limits.

CB5.3.1

The application should be subject to an information risk analysis, performed in compliance with enterprise-wide standards / procedures for information risk analysis, using a structured Information Risk Analysis Methodology.

Information risk analysis (sometimes referred to as simply risk analysis or risk assessment) is the identification, measurement and prioritisation of risk, and the selection of security controls to mitigate that risk. An example of a structured methodology is the ISF's Information Risk Analysis Methodology (IRAM).

CB5.3.2

The information risk analysis should involve:

a) the business owner of the application
b) an IT specialist
c) key user representatives
d) an expert in risk analysis (eg a member of staff or a third party specialist who has significant experience as an information risk analysis practitioner)
e) an information security specialist (eg a member of staff or a third party specialist who has significant experience as an information security practitioner).

CB5.3.3

The information risk analysis should determine risk by assessing:

a) the potential level of business impact associated with the application
b) accidental and deliberate threats to the confidentiality, integrity or availability of information (eg denial of service attacks, malware, misusing systems to commit fraud, loss of power, malfunctions and human error) stored in or processed by the application
c) vulnerabilities due to control weaknesses
d) vulnerabilities due to circumstances that increase the likelihood of a serious information security incident occurring (eg use of the Internet, permitting third party access or siting a computer installation in an area prone to earthquakes or flooding).

CB5.3.4

The information risk analysis should take into account:

a) compliance requirements (eg legislation, regulation, industry standards and internal policies)
b) objectives of the organisation
c) information classification requirements
d) previous risk analyses conducted on the application being assessed
e) characteristics of the operating environment of the application, network or computer installation being assessed.

(continued on the next page)

Section CB5.3 Information risk analysis (continued)

CB5.3.5

Results of the information risk analysis should be documented and include:

a) a clear identification of key risks
b) an assessment of the potential business impact of each risk
c) recommended actions to reduce risks to an acceptable level.

CB5.3.6

The information risk analysis process should be used to help:

a) select information security controls that will reduce the likelihood of serious information security incidents occurring
b) select information security controls that will satisfy relevant compliance requirements (eg the Sarbanes-Oxley Act 2002, the Payment Card Industry (PCI) Data Security Standard, Basel II 1998, data privacy requirements and anti-money laundering laws)
c) determine the costs of implementing security controls (eg costs associated with: design, purchase, implementation and monitoring of the controls; hardware and software; training; overheads, such as facilities; and consultancy fees)
d) evaluate the strengths and weaknesses of security controls
e) identify specialised security controls required by the application (eg data encryption or strong authentication).

CB5.3.7

Results of the information risk analysis (including risk treatment actions and any identified residual risk) should be:

a) communicated to the application owner and top management (eg board-level executives or equivalent)
b) signed off by an appropriate business representative.

Risk treatment typically involves one of four options: applying appropriate controls; accepting risks; avoiding risks; or transferring risks. Residual risk is that proportion of risk that still remains after selected controls have been implemented.

CB5.3.8

Information risk analyses of the application should be performed regularly and before major changes to the application are implemented.

Section CB5.4 Security audit / review

Principle The information security status of the application should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls have been implemented effectively, that information risk is being managed, and to provide the application owner and top management with an independent assessment of the information security status of the application.

CB5.4.1

Security audits / reviews of the application should be performed regularly and carried out independently of staff involved with running or supporting the application (eg by a third party specialist or by internal audit).

CB5.4.2

Security audits / reviews should:

a) assess the business risks associated with the application
b) consider the information security requirements of the application.

CB5.4.3

Security audits / reviews of the application should assess the status of information security arrangements in key areas (eg application management, the end user environment, system management and special topics, such as third party access, cryptographic key management and web-enabled technology).

CB5.4.4

Security audits / reviews of the application should be:

a) agreed with the application owner
b) defined in scope, and documented
c) performed by experienced and qualified individuals who have sufficient technical skills and knowledge of information security
d) conducted frequently and thoroughly (in terms of scope and extent) to provide assurance that security controls function as required
e) focused on ensuring that controls are effective enough to reduce risks to acceptable levels
f) supplemented by the use of automated software tools
g) validated by competent individuals
h) complemented by reviews carried out by independent third parties.

CB5.4.5

Security audit / review activity should be managed by:

a) agreeing requirements for special processing routines or tests (eg network and application penetration testing) with an appropriate business representative
b) restricting access to the application by the audit / review team (eg by granting only 'read' access to business information and software files or other types of access only for isolated copies of business information and software files)
c) monitoring and logging the activities of the audit / review team
d) disposing of business information copied for the purpose of audit / reviews as soon as it is no longer required (eg by erasure or physical destruction)
e) protecting software tools used in carrying out audits / reviews (eg by keeping them separate from tools / utilities used in the live environment and holding them in secure storage facilities, such as restricted software libraries)
f) protecting documents and system files relating to the audit / review.

(continued on the next page)

Section CB5.4 Security audit / review (continued)

CB5.4.6

Recommendations following security audits / reviews should be agreed with the application owner, and reported to top management (eg board-level executives or equivalent).

Area CB6
SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns. Where these topics apply to a critical business application, special security arrangements are required. Accordingly, this area covers the additional security controls required by applications that provide third party access, employ cryptographic key management, use a public key infrastructure (PKI) or are based on web-enabled technology.

Section CB6.1 Third party agreements

Principle Connections from third parties (ie external organisations, such as customers, suppliers and members of the public) should be subject to an information risk analysis, approved by the application owner and agreed by both parties in a documented agreement, such as a contract.

Objective To ensure that only approved third parties are granted access to the application.

CB6.1.1

Third party access arrangements should be reviewed regularly to ensure that risks remain within an acceptable limit. The review should take account of the:

a) criticality of information and systems to be accessed
b) sensitivity of information and systems to be accessed
c) relationship with third parties to be granted access (from well-known, established trading partners to new, unknown organisations)
d) types of business process to be performed or supported by third parties (eg information retrieval, order submission, funds transfer or remote maintenance)
e) effectiveness of the IT infrastructure in restricting third parties to agreed capabilities
f) technical aspects of connection (eg access control mechanisms and methods of connections, such as broadband or ISDN)
g) vulnerabilities in third party networks, operating systems or applications
h) restrictions imposed by legal or regulatory requirements (eg Basel II 1998, Sarbanes-Oxley Act and the Payment Card Industry (PCI) Data Security Standard)
i) lack of direct control over staff or system components employed by third parties
j) obligations to third parties (eg to provide a reliable service and supply timely, accurate information)
k) information security practices and standards of third parties (eg by reviewing their information security policies).

CB6.1.2

The provision of third party access should be supported by documented agreements, and signed off by an appropriate business representative (eg the individual in charge of a business process or activity). Agreements should oblige third parties to comply with good practice for information security (eg the ISF's Standard of Good Practice or ISO/IEC 27002 (17799)) and provide details about potential and actual information security incidents.

(continued on the next page)

Section CB6.1 Third party agreements (continued)

CB6.1.3

Third party agreements should cover management activities, which include:

a) arrangements for managing changes to the application
b) preparing for and managing information security incidents
c) the right to audit and monitor security arrangements within the third party
d) timeframes for completion of transactions (eg processing sales order requests, changing inventory levels, recording manufacturing statistics and updating production schedules) and arrangements for ensuring that transactions cannot be repudiated (eg by using 'digital signatures')
e) the respective liabilities of the parties to the agreement
f) protection of intellectual property rights, copyright assignment and collaborative work
g) the right to monitor and revoke user activity
h) details about ownership of the information covered by the agreement
i) actions to be taken in the event of a breach of the agreement
j) the need for information security awareness
k) maintenance of documentation (eg asset lists and software licences).

CB6.1.4

Third party agreements should cover information security activities, which include:

a) details of the confidentiality, integrity and availability requirements of information covered by the agreement
b) agreed security controls (eg access mechanisms, malware protection and back-up)
c) non-disclosure of information gained in the course of work
d) a requirement to return or destroy information or software on an agreed date, or upon request
e) how information can be used (eg the processing, storing and exchange of information with additional third parties)
f) arrangements for the protection of important information (eg cryptographic keys and software).

CB6.1.5

There should be a method for managing changes to third party agreements (eg to support renegotiation activities).

Section CB6.2 Cryptographic key management

Principle Cryptographic keys should be managed tightly, in accordance with documented standards / procedures, and protected against unauthorised access or destruction.

Objective To ensure that cryptographic keys are not compromised (eg through loss, corruption or disclosure).

CB6.2.1

There should be documented standards / procedures for managing cryptographic keys, which cover:

a) generation of cryptographic keys, using approved key lengths
b) secure distribution, storage, recovery and replacement / update of cryptographic keys
c) revocation of cryptographic keys (eg if a key is compromised, or a key owner changes job or leaves the organisation)
d) recovery of cryptographic keys that are lost, corrupted or have expired
e) management of cryptographic keys that may have been compromised, such as by disclosure to a third party
f) back-up / archive of cryptographic keys and the maintenance of cryptographic key history
g) allocation of defined activation / de-activation dates
h) restriction of access to cryptographic keys to authorised individuals
i) sharing of cryptographic keys (eg using split key generation) required for protecting sensitive information and critical systems.

Cryptographic keys can be used to protect the confidentiality of information, preserve its integrity, provide strong authentication, and support non-repudiation (ie to enable the identity of the originator of information to be proven).

CB6.2.2

Individuals who clearly understand their responsibilities should be assigned to manage cryptographic keys.

CB6.2.3

Cryptographic keys should be protected against:

a) unauthorised access
b) destruction.

Section CB6.3 Public key infrastructure

Principle Any public key infrastructure (PKI) used by the application should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.

Objective To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

CB6.3.1

For an application that uses a public key infrastructure (PKI), documented standards / procedures should be established (eg a Certification Practice Statement (CPS) and one or more corresponding Certificate Policies (CP)), which define the:

a) process required to manage cryptographic keys / digital certificates associated with the PKI
b) methods required to operate the PKI
c) actions to be taken in the event of a compromise or suspected compromise of the PKI (eg revocation of the Root Certification Authorities (CA), digital certificates and any sub-CAs).

A Certification Authority (CA) comprises the people, processes and tools that are responsible for the creation, issue and management of public key certificates that are used within a PKI.

CB6.3.2

Users of the public key infrastructure should be made aware of the purpose and function of the PKI and their responsibilities (eg to protect private keys, and how to use digital signatures).

CB6.3.3

Internal Certification Authorities should be protected by:

a) restricting access to the Certification Authority (eg by using access control mechanisms and strong authentication)
b) 'hardening' the operating system(s) that support the Certification Authority (eg by removing all known vulnerabilities, disabling unnecessary services and changing vendor supplied passwords)
c) employing other general controls (eg change management, back-up and security event logging) in a particularly disciplined manner.

CB6.3.4

Contingency plans for the application supported by the PKI should include methods of recovering the PKI in the event of a disaster.

Section CB6.4 Web-enabled applications

Principle Specialised procedural and technical controls should be applied to web-enabled applications and the servers on which they run.

Objective To ensure that the increased risks associated with web-enabled applications are minimised.

CB6.4.1

The business practices and privacy policies applicable to the website(s) associated with the application should be independently accredited (eg by organisations such as Web Trust, TRUSTe or equivalent).

CB6.4.2

Web servers that support the application should be:

a) segregated from internal networks and untrusted networks (eg in a 'Demilitarised Zone' (DMZ))
b) run on one or more dedicated computers (ie they do not provide other services such as file and print, database or e-mail or other business applications)
c) run with 'least privilege' (eg excluding the use of high-level privileges, such as 'root' for UNIX systems or 'Administrator' for Windows systems)
d) prevented from initiating network connections to the Internet (eg through server configuration or by rules on a firewall)
e) configured so that scripts can only be run from specified locations
f) reviewed to ensure that all unnecessary software, network services and applications have been disabled / removed
g) configured to log security-related events generated by the website.

CB6.4.3

Connections between web servers and back-office systems (eg application and database servers) should be:

a) protected by firewalls (eg stateful inspection firewalls (typically located in the perimeter of a network), application proxy firewalls (typically located between internal networks) and application firewalls (typically located close to the application))
b) restricted to services that are essential to the application
c) restricted to those originating from web server applications (ie rather than originating from client applications)
d) based on documented, tested and approved application programming interfaces (APIs)
e) supported by mutual authentication (ie two computers verifying each other's identity before exchanging data).

CB6.4.4

User accounts that are used by web servers to make connections to back-office systems should run with 'least privilege' (eg excluding the use of high-level privileges, such as 'root' for UNIX systems or 'Administrator' for Windows systems).

CB6.4.5

Information used by the application should be protected against corruption or disclosure by:

a) performing input validation at the server, rather than just on the client application
b) encrypting sensitive information in transit (eg by using Secure Sockets Layer (SSL) or Transport Layer Security (TLS))
c) protecting files containing connection settings (eg used to connect to back-end systems) against loss, corruption or disclosure, by locating them on partitions inaccessible to the website and by restricting permissions.

(continued on the next page)

Section CB6.4 Web-enabled applications (continued)

CB6.4.6

Website content should be:

a) stored on a separate partition / disk from the operating system
b) protected by setting file permissions
c) updated by authorised individuals and using approved methods (eg via CD at the web server console or transferring files using secure shell (SSH) or secure FTP from a predefined IP address)
d) reviewed to ensure that it is accurate, that hyperlinks are valid and functional, and that vulnerabilities have not been introduced by scripts or 'hidden' form fields.

CB6.4.7

Checks should be performed regularly to ensure that website content is not defamatory, offensive or in breach of legal and regulatory requirements.

Computer Installations

Computer installations typically support critical business applications and safeguarding them is, therefore, a key priority. Since the same information security principles apply to any computer installation (irrespective of where, or on what scale or types of computer it takes) a common standard of good practice for information security should be applied.

Computer Installations

CI1 Installation Management

CI1.1 Roles and responsibilities

CI1.2 Service agreements

CI1.3 Asset management

CI1.4 System monitoring

CI2 Live Environment

CI2.1 Installation design

CI2.2 Security event logging

CI2.3 Host system configuration

CI2.4 Workstation protection

CI2.5 Resilience

CI2.6 Hazard protection

CI2.7 Power supplies

CI2.8 Physical access

CI3 System Operation

CI3.1 Handling computer media

CI3.2 Back-up

CI3.3 Change management

CI3.4 Information security incident management

CI3.5 Emergency fixes

CI3.6 Patch management

CI4 Access Control

CI4.1 Access control arrangements

CI4.2 User authorisation

CI4.3 Access privileges

CI4.4 Sign-on process

CI4.5 User authentication

CI5 Local Security Management

CI5.1 Local security co-ordination

CI5.2 Security awareness

CI5.3 Information classification

CI5.4 Information risk analysis

CI5.5 Security audit / review

CI6 Service Continuity

CI6.1 Contingency plans

CI6.2 Contingency arrangements

CI6.3 Validation and maintenance

Area CI1
INSTALLATION MANAGEMENT

Computer installations used for processing information need to be well managed. Accordingly, this area covers the roles and responsibilities of the staff involved in running computer installations, agreements made with business users, management of key assets (eg hardware and software) and monitoring of the systems associated with the installation.

Section CI1.1 Roles and responsibilities

Principle An owner should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To achieve individual accountability for the computer installation, provide a sound management structure for staff running the installation and give responsible individuals a vested interest in its protection.

CI1.1.1

An owner should be assigned for managing the computer installation. Responsibilities for key tasks should be clearly assigned to one or more capable individuals, who should accept the responsibilities (including those for information security) associated with these roles.

CI1.1.2

Individuals who run the computer installation should be:

a) competent to deal with normal processing requirements
b) able to deal with error, exception and emergency conditions
c) sufficient in number to handle normal and peak workloads.

CI1.1.3

The risk of staff disrupting the running of the installation either in error or by malicious intent should be reduced by:

a) separating the duties of staff running the installation from the duties of development and testing staff
b) ensuring internal staff and external individuals (eg consultants, contractors, engineers) sign non-disclosure / confidentiality agreements
c) minimising reliance on key individuals (eg by automating processes, ensuring supporting documentation is complete and accurate, and arranging alternative cover for key roles)
d) organising duties in such a way as to minimise the risk of theft, fraud, error and unauthorised changes to information (eg by supervising and recording activities, prohibiting lone working and the segregation of duties)
e) screening applicants for positions that involve running the installation (eg by taking up references, checking career history / qualifications and confirming identity by inspecting a passport).

CI1.1.4

There should be documented standards / procedures that apply to the computer installation, which are:

a) consistent with policies that apply enterprise-wide
b) communicated to staff involved in running the installation
c) approved by an appropriate business representative, reviewed regularly and kept up-to-date.

Section CI1.2 Service agreements

Principle Users' service requirements should be classified in a way that identifies their criticality to the business, and documented in contracts or service level agreements.

Objective To define the business requirements, including information security requirements, for services provided by the computer installation.

CI1.2.1

Users' service requirements should be documented in agreements, such as contracts or service level agreements (SLAs).

A service level agreement (SLA) should include all key elements, such as: who is in charge of the application (ie the application owner); who is in charge of delivering the required service (eg an internal or external service provider); capacity requirements; maximum permissible down-time; and criteria for measuring the level of service.

CI1.2.2

Service agreements should specify:

a) the business owner(s) of applications supported by the installation
b) who is responsible for delivering the required service
c) the level of criticality of the service
d) dates / times when the service is required
e) capacity requirements (eg the projected number of users, volumes of work to be handled, response times and transmission rates)
f) maximum processing response times
g) critical timescales (ie the timescale beyond which a loss of service would be unacceptable to the organisation).

CI1.2.3

Service agreements should cover:

a) arrangements for ensuring continuity of service (eg duplication of computers, storage media and communications links)
b) access controls to be applied to the installation
c) cryptographic controls to be used in the installation (eg to encrypt files, authenticate users or preserving the integrity of information)
d) protection against malware (eg computer viruses, worms, trojan horses, spyware, adware and malicious mobile code)
e) segregation of duties and facilities (including business users, applications, computers and networks)
f) change management and information security incident management
g) back-up and archiving
h) installation and maintenance activity relating to hardware and software.

Malware typically includes computer viruses, worms, trojan horses, spyware, adware and malicious mobile code (executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions).

(continued on the next page)

Section CI1.2 Service agreements (continued)

CI1.2.4

The conditions of service agreements should be enforced, and reviewed regularly.

CI1.2.5

Arrangements should be made with the service provider to deal with security issues via a single point of contact (eg a helpdesk or service desk) and through an individual who is sufficiently senior and competent to deal with security issues effectively.

Section CI1.3 Asset management

Principle Essential information about hardware and software (eg unique identifiers, version numbers and physical locations) should be recorded in inventories, and software licensing requirements met.

Objective To protect information stored in or processed by the computer installation and to meet legal / regulatory requirements.

CI1.3.1

There should be documented standards / procedures for asset management that apply to the computer installation, which cover the need to:

a) record important information about different types of hardware and software in an inventory (or equivalent)
b) protect the inventory and keep it up-to-date
c) meet software licensing requirements.

CI1.3.2

Important information about hardware and software (including computer equipment, application / system software, and critical desktop applications) should be recorded in inventories (eg an asset register).

Critical desktop applications are typically developed using spreadsheet and database programs, and used to support critical business processes, such as processing high-value transactions, analysing financial information, performing business modelling and managing important production information.

Critical desktop applications can range in complexity from basic lists or simple calculations to complex calculations.

CI1.3.3

Inventories should specify:

a) a unique description of hardware and software in use
b) versions of hardware and software in use
c) the location of hardware and software in use.

CI1.3.4

Inventories should be:

a) protected against unauthorised change
b) checked regularly against actual assets (eg physical assets or software licensing agreements) to help identify gaps in registers and unauthorised copies of software
c) kept up-to-date
d) reviewed independently.

CI1.3.5

Software licensing requirements should be met by obtaining adequate licenses for planned use and providing proof of ownership (eg via 'blanket' licence agreements).

Section CI1.4 System monitoring

Principle Systems associated with the computer installation should be monitored continuously, and reviewed from a business user's perspective.

Objective To assess the performance of the computer installation, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

CI1.4.1

The performance of systems associated with the computer installation should be monitored:

a) against agreed targets
b) by reviewing current utilisation of systems at normal and peak periods
c) using automated monitoring software
d) by reviewing event logs of system activity regularly (eg to help identify suspicious or unauthorised activity)
e) by investigating bottlenecks / overloads.

CI1.4.2

Key information relating to system monitoring should be retained long enough to meet legal / regulatory requirements (eg by archiving the information to removable media and storing it in a safe location).

CI1.4.3

Capacity planning activities should be undertaken to allow extra capacity to be commissioned before projected bottlenecks / overloads materialise.

CI1.4.4

System availability (ie response and up-time) should be measured from the perspective of business users (eg by monitoring workstation performance).

CI1.4.5

System monitoring activities should be conducted regularly, and involve:

a) scanning host systems (eg using automated tools such as Nessus, Pingware, SATAN or ISS Safesuite) for known vulnerabilities
b) checking whether powerful utilities / commands have been disabled on attached hosts (eg by using a 'network sniffer')
c) checking for the existence and configuration of unauthorised wireless networks (eg using automated tools such as Netstumbler, KISMET and Airsnort)
d) discovering the existence of unauthorised systems (eg by using network discovery and mapping tools)
e) detecting unauthorised changes to electronic documents and configuration files (eg by using file integrity monitoring software).

CI1.4.6

Intrusion detection mechanisms should be employed, which include:

a) detection of known attack characteristics (eg denial of service and buffer overflows)
b) detection of unusual system behaviour (eg identifying anomalies in standard protocols)
c) a process to incorporate new or updated attack characteristics
d) provision of alerts when suspicious activity is detected, supported by documented processes for responding to suspected intrusions
e) protection of intrusion detection software against attack (eg by hiding the presence of intrusion detection software).

(continued on the next page)

Section CI1.4 System monitoring (continued)

CI1.4.7

Usage reports from service providers (eg invoices or service reports) should be examined to discover any unusual use of the systems within the installation (eg by reviewing patterns of activity).

CI1.4.8

The results of monitoring activities should be reviewed by the installation owner and presented to the application owner(s) to whom services are provided.

Area CI2
LIVE ENVIRONMENT

Service targets are more likely to be achieved if computer installations are designed well. Accordingly, this area covers the design of the installation, logging of key security-related events and the configuration of host systems and workstations. It also covers the resilience of the installation and its protection from physical loss or damage.

Section CI2. 1 Installation design

Principle Computer installations should be designed to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.

Objective To produce a computer installation that has security functionality built-in and enables additional controls to be incorporated easily.

CI2.1.1

There should be documented standards / procedures for installation design, which require the:

a) design to take account of users' service requirements and be consistent with other installations used by the organisation
b) installation to be designed to cope with foreseeable developments in the organisation's use of IT (eg growth projections or adoption of open / proprietary standards).

CI2.1.2

The installation should be designed to:

a) support consistent naming conventions (eg computer / server addresses, terminal locations and user identifiers)
b) be managed from a single point (eg an operations centre)
c) enable authorised users to access multiple systems and resources via reduced sign-on, and be administered from a single point
d) minimise the need for manual intervention (eg by incorporating high-reliability or fault-tolerant computers and automating common operations such as patch management and back-up)
e) include the installation of malware protection software on key servers
f) enable a standard predetermined server configuration to be built, which can be automated (eg a standard build).

CI2.1.3

Live environments should be segregated from development and acceptance testing activity by storing system utilities away from the live environment when not in use and by using different computer rooms, processors, domains and partitions.

CI2.1.4

Key components of the installation should be protected by:

a) segregating critical business applications from all other business applications and information, as agreed with their business owners
b) storing source code (or equivalent) in a secure location away from the live environment and restricting access to authorised individuals
c) segregating different types of software and information (eg by storing them in separate directories)
d) permitting only execute access to executable software (eg run-time code, stored procedures or CGI scripts).

Section CI2.2 Security event logging

Principle Important security-related events should be recorded in logs, stored centrally, protected against unauthorised change and analysed on a regular basis.

Objective To identify threats that may lead to an information security incident, and maintain the integrity of important security-related information.

CI2.2.1

There should be documented standards / procedures for security event logging that apply to the computer installation.

CI2.2.2

Standards / procedures should cover:

a) management of security event logging (eg setting policy, defining roles and responsibilities, signing off budget and reporting)
b) identification of systems on which event logging should be enabled to help identify security-related events (eg critical business systems, systems that have experienced a major information security incident, or systems that are subject to legislative or regulatory mandates)
c) configuration of systems to generate security-related events (including event types such as failed log-on, system crash, deletion of user account and event attributes such as date, time, UserID, file name, IP address)
d) storage of security-related events within event logs (eg using local systems, central servers, or by using storage provided by a third party service provider)
e) protection of security-related event logs (eg via encryption, access control and back-up)
f) analysis of security-related event logs (including normalisation, aggregation and correlation)
g) retention of security-related event logs (eg to meet legal, regulatory and business requirements for possible forensic investigations).

CI2.2.3

Security event log management should include: setting policy; defining roles and responsibilities; ensuring the availability of relevant resources and guidance on the frequency and content of reports.

CI2.2.4

Security event logging should be performed on systems that:

a) are critical to the organisation (eg financial databases, servers storing medical records or key network devices)
b) have experienced a major information security incident
c) are subject to legislative or regulatory mandates.

CI2.2.5

Host systems should be configured to:

a) enable event logging
b) generate appropriate event types (eg system crash, object deletion and failed logon attempts)
c) incorporate relevant event attributes in event entries (eg IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name)
d) use a consistent and correct system date and time (eg by establishing a network time server and using the network time protocol (NTP)).

(continued on the next page)

Section CI2.2 Security event logging (continued)

CI2.2.6

Security-related event logging should be:

a) enabled at all times
b) protected from accidental or deliberate overwriting.

CI2.2.7

Mechanisms should be established so that when event logs reach a maximum size, the system is not halted through lack of disk space and logging continues with no disruption.

CI2.2.8

Security-related event logs should be analysed regularly (eg using automated tools), and include:

a) processing of key security-related events (eg using techniques such as normalisation, aggregation and correlation)
b) interpreting key security-related events (eg identification of unusual activity)
c) responding to key security-related events (eg passing the relevant event log details to an information security incident management team).

CI2.2.9

Security-related event logs should be:

a) retained according to retention standards / procedures
b) copied on to removable storage media that can preserve the event log information (in electronic format) for long periods of time
c) stored securely for possible forensic analysis at a later date.

Section CI2.3 Host system configuration

Principle Host systems should be configured to function as required, and to prevent unauthorised or incorrect updates.

Objective To ensure host systems operate as intended and do not compromise the security of the computer installation.

CI2.3.1

Host systems should be configured in accordance with documented standards / procedures, which should cover:

a) disabling or restricting particular functions or services
b) restricting access to powerful system utilities and host parameter settings (eg Windows Registry Editor)
c) using time-out facilities
d) performing key software updates (eg patches and security fixes).

CI2.3.2

Host systems should be configured to disable or restrict:

a) non-essential or redundant services (eg X Windows, Open Windows, fingerd and web browsers)
b) communication services that are inherently susceptible to abuse (eg tftp, RPC, rlogin, rsh or rexec)
c) communication protocols that are prone to abuse (eg DNS, FTP, NNTP, RIP, SMTP, Telnet and UUCP)
d) execute permissions on sensitive commands or scripts (eg rlogin, rcp, rsh, remsh, tstp and trtp)
e) powerful utilities (eg Windows 'Registry Editor') or 'control panels'
f) 'run' commands or command processors (eg Perl or Tcl).

CI2.3.3

Access to powerful system utilities and host system parameter settings should be:

a) restricted to a limited number of trusted individuals
b) restricted to narrowly-defined circumstances (eg for the duration of an authorised change)
c) subject to individual authorisation (eg by the person in charge of the installation).

CI2.3.4

Host systems should be protected against unauthorised access by:

a) disabling unnecessary or insecure user accounts (eg the 'Guest' account (or equivalent) for Windows XP and UNIX systems)
b) changing important security-related parameters (eg passwords) to be different from the defaults set by suppliers
c) invoking time-out facilities that automatically logoff workstations after a set period of inactivity, clear screens and require users to sign-on again before restoring screens.

CI2.3.5

Technical vulnerabilities in software should be identified and evaluated to determine applicability and potential business impact.

CI2.3.6

Security patches or fixes to address vulnerabilities should be:

a) identified quickly (eg by tracking CERT alerts, vendor websites and mailing lists)
b) evaluated to determine the potential business impact of applying the patch
c) tested, and applied in a timely manner.

Section CI2.4 Workstation protection

Principle Workstations connected to systems within the computer installation should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements, and protected by physical and logical controls.

Objective To ensure workstations operate as intended and do not compromise the security of the systems to which they are connected.

CI2.4.1

Workstations (ie desktop computers and laptop computers) connected to systems running in the installation should be supported by documented standards / procedures, which cover:

a) implementation and maintenance of workstations
b) provision of security software to protect workstations (eg system management tools, access control mechanisms, malware protection software and encryption capabilities)
c) software configuration of workstations (eg employing standard builds and relevant web browser settings)
d) protection against malicious mobile code (eg executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that have been written deliberately to perform unauthorised functions).

CI2.4.2

Workstations should be:

a) purchased from approved suppliers (ie those with a proven record of providing robust and resilient equipment)
b) tested prior to use
c) supported by maintenance arrangements
d) protected by physical and environmental controls
e) provided with standard technical configurations (eg running a standard operating system, standard applications and common communications software).

CI2.4.3

Workstations should be protected by the use of:

a) a comprehensive set of system management tools (eg maintenance utilities, remote support, organisation management tools and back-up software)
b) access control mechanisms (ie to restrict access to the workstation)
c) up-to-date malware protection software, to protect against malicious software (eg computer viruses, worms, trojan horses, spyware, adware and malicious mobile code)
d) encryption software to safeguard information stored on internal and external hard disk drives
e) automatic time-out after a set period of inactivity
f) restrictions on the use of removable storage media (eg prohibition of personal use of external hard disk drives and USB memory sticks).

Malware typically includes computer viruses, worms, trojan horses, spyware, adware and malicious mobile code (executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions).

(continued on the next page)

Section CI2.4 Workstation protection (continued)

CI2.4.4

Portable devices (eg laptop computers and Personnel Digital Assistants (PDAs)) should be protected against theft by:

a) providing users with physical locks or equivalent security devices
b) attaching identification labels
c) the use of indelible marking.

CI2.4.5

Workstations that can connect to the Internet should be protected by:

a) using web browsers with a standard, secure configuration
b) preventing users from disabling security options in web browsers
c) applying updates to web browser software quickly and efficiently
d) using personal firewalls
e) warning users of the dangers of downloading mobile code and of the implications of accepting or rejecting 'cookies' (small text files containing information that can be used to identify a user returning to a website)
f) restricting the downloading of mobile code (eg executable code such as Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions).

Section CI2.5 Resilience

Principle The computer installation should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective To ensure that the systems supported by the computer installation are available when required.

CI2.5.1

Components that are critical to the functioning of the computer installation should be identified and recorded in an inventory, or equivalent.

CI2.5.2

Resilience of the installation should be improved by providing duplicate or alternative:

a) hardware components (eg servers, processors, hard disk drives, network interface cards and memory) to create fault tolerant systems
b) data storage facilities (eg disk mirroring and RAID technology)
c) locations from which the installation can be run in an emergency
d) network devices.

CI2.5.3

When acquiring hardware / software:

a) products should be selected from a list of approved suppliers
b) security requirements should be considered
c) high priority should be given to reliability
d) contractual terms should be agreed with suppliers.

CI2.5.4

The risk of potential security weaknesses in hardware / software should be reduced by:

a) obtaining external assessments from trusted sources (eg auditors' opinions and specified security criteria, such as the 'Common Criteria' and Federal Information Processing Standards (FIPS))
b) identifying security deficiencies (eg by detailed inspection, reference to published sources, or by participating in user / discussion groups)
c) considering alternative methods of providing the required level of security (eg 'work-arounds').

CI2.5.5

The resilience of the installation should be improved by:

a) using proven equipment, software and services
b) servicing equipment in accordance with manufacturers' recommended service intervals
c) maintaining an adequate supply of system consumables (eg printer ribbons and cartridges, stationery, data storage media)
d) prohibiting servicing of equipment by unqualified individuals
e) recording all faults or suspected faults
f) disabling equipment, software and services with suspected faults until remedied
g) keeping equipment and software up-to-date and maintaining change management disciplines
h) maintaining up-to-date back-ups of the software, control tables and settings used in the installation
i) ensuring equipment that is critical to the functioning of the installation or particularly susceptible to failure can be replaced quickly (eg by holding a stock of spares on-site)
j) ensuring timely repair of equipment is achieved through agreements with specialist service providers.

Section CI2.6 Hazard protection

Principle Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.

Objective To prevent services being disrupted by damage to computer equipment or facilities caused by fire, flood and other types of hazard.

CI2.6.1

The computer installation should be located in a safe environment (eg in an area with low risk of fire, flood, explosion, civil unrest, damage from neighbouring activities or natural disasters) and in rooms protected from natural hazards.

CI2.6.2

Rooms housing critical IT facilities should be:

a) free from intrinsic fire hazards (such as paper or chemicals)
b) fitted with fire detection and suppression systems
c) protected against the spread of fire (eg by using fire resistant doors).

CI2.6.3

Fire alarms should be monitored continuously, tested regularly and serviced in accordance with manufacturer specifications.

CI2.6.4

The impact of hazards should be minimised by:

a) locating hand-held fire extinguishers so that minor incidents can be tackled without delay
b) training staff in the use of fire extinguishers and other emergency / safety equipment, and in emergency evacuation procedures
c) protecting computer equipment against damage from environmental hazards (eg smoke, dust, vibration, chemicals, electrical interference / radiation, food, drink and nearby industrial processes)
d) monitoring and controlling the temperature and humidity of computer rooms in accordance with equipment manufacturer recommendations.

Section CI2.7 Power supplies

Principle Critical computer equipment and facilities should be protected against power outages.

Objective To prevent services provided by the computer installation from being disrupted by loss of power.

CI2.7.1

Power cables within the computer installation should be protected by:

a) segregating them from communications cables to prevent interference
b) concealed installation
c) locked inspection / termination points
d) alternative feeds or routing
e) avoidance of routes through public areas.

CI2.7.2

The power supply to critical computer equipment should be protected by:

a) using uninterruptible power supply (UPS) devices and surge protection equipment (eg lightning protection filters and radio frequency interference (RFI) filters)
b) providing back-up generators (supplied with adequate quantities of fuel) in case of extended power failure
c) installing emergency lighting in case of main power failure
d) siting emergency power-off switches near emergency exits to facilitate rapid power-down in case of an emergency.

CI2.7.3

Emergency equipment (eg UPS equipment, back-up generators and lighting) should be serviced in accordance with manufacturer recommendations and tested regularly.

Section CI2.8 Physical access

Principle Physical access to critical computer installation facilities should be restricted to authorised individuals.

Objective To prevent services being disrupted by loss of or damage to equipment or facilities.

CI2.8.1

Physical access to the computer installation should be restricted to authorised individuals by:

a) installing locks activated by key pads, swipe cards or equivalent
b) locking doors / windows when the environment is vacated
c) fitting intruder alarms
d) ensuring all individuals wear visible means of identification
e) requiring staff to challenge strangers
f) employing security guards.

CI2.8.2

Within the installation:

a) physical access to post / facsimile points and equipment used for sensitive printed material should be restricted
b) sensitive media and documentation should be locked away when not in use (eg as part of a 'clear desk' policy)
c) intruder detection systems installed on external doors and accessible windows should be tested regularly
d) easily-portable computers and components (eg laptop computers, wireless access points, external hard disk drives, USB memory sticks and printers) should be protected against theft (eg by indelibly marking vulnerable equipment or fastening computers to desks or equipment stands).

CI2.8.3

Visitors to the installation should be:

a) permitted access only for defined and authorised purposes
b) monitored by recording arrival and departure times
c) supervised at all times
d) issued with instructions explaining the security requirements of the area, detailing emergency procedures and stating that audio and video recording (eg filming or photography) is prohibited.

CI2.8.4

Individuals should be required to obtain written approval before leaving the environment with computer equipment (eg servers, workstations, network devices and printers) or equivalent.

CI2.8.5

Critical equipment and facilities should be protected by locating them away from public access or approach and keeping details about them confidential (eg by using discreet signs or excluding details from directories or telephone books).

CI2.8.6

Identification labels should be attached to equipment owned by the organisation (eg desktop computers, laptop computers, hand-held computing devices such as Personnel Digital Assistant (PDAs) and network devices such as wireless access points).

(continued on the next page)

Section CI2.8 Physical access (continued)

CI2.8.7

Physical access to rooms housing critical equipment and facilities should be protected by:

a) defining and strengthening the physical security perimeter (eg by using solid construction walls, alarmed fire doors, armoured windows and physical barriers)
b) keeping rooms under constant surveillance (eg using closed-circuit television (CCTV))
c) siting computer equipment (eg server console screens, workstations and printers) so that sensitive information cannot be overlooked
d) isolating the holding area for receipt of deliveries from other parts of the installation.

CI2.8.8

Authorisation to gain physical access to the installation should be:

a) issued in accordance with documented standards / procedures
b) reviewed regularly, to ensure that only appropriate individuals are allowed access
c) revoked promptly when no longer needed.

Area CI3
SYSTEM OPERATION

Achieving service targets requires computer installations to be run in accordance with sound disciplines. Accordingly, this area covers basic controls over system operation (ie handling computer media, back-up and change management) and arrangements for identifying and resolving incidents (ie information security incident management and emergency fixes).

Section CI3.1 Handling computer media

Principle Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure, and additional security controls applied to media containing sensitive information.

Objective To protect computer media in accordance with information security and regulatory requirements.

CI3.1.1

There should be documented standards / procedures for handling data storage media (including magnetic tapes, disks, printed results, and stationery).

CI3.1.2

The information held on data storage media should be protected by:

a) erasing the content of reusable data storage media when no longer needed
b) storing data storage media in accordance with manufacturer specifications
c) recording and approving the transfer of files using data storage media
d) keeping records of data storage media taken outside the environment in which they are normally used
e) removing business information from data storage media prior to sending computers off-site for maintenance.

CI3.1.3

There should be documented standards / procedures for handling and disposing of sensitive material (eg blank cheques, print-outs of personally identifiable information and removable storage media containing sensitive information, such as financial projections or business plans) associated with the installation.

CI3.1.4

Sensitive material should be protected when handled by:

a) labelling material to reflect its sensitivity and information classification
b) minimising distribution
c) recording authorised recipients and clearly marking all information with the identity of the authorised recipient
d) confirming receipt of transmitted data and reviewing records of authorised recipients regularly
e) checking completeness of sensitive material (eg by ensuring all information is input and processed, and that there is proper accounting for all computer media).

CI3.1.5

Sensitive documents and data storage media should be stored in physically secure locations (eg locked, document or computer media fireproof safes).

(continued on the next page)

Section CI3.1 Handling computer media (continued)

CI3.1.6

Sensitive data storage media and printed material should be protected when being disposed by:

a) using secure means of disposal (eg erasure, incineration or shredding)
b) recording its disposal
c) checking that information stored data storage media has been erased prior to disposal.

Section CI3.2 Back-up

Principle Back-ups of essential information and software used by the computer installation should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential information and software required by the installation can be restored within critical timescales.

CI3.2.1

Back-ups of essential information and software used by the computer installation (eg business information, systems information and application information) should be performed frequently enough to meet business requirements.

CI3.2.2

There should be documented standards / procedures for performing back-ups, which cover:

a) the types of information to be backed-up
b) back-up cycles
c) methods for performing back-ups (including validation, labelling and storage).

CI3.2.3

Back-up processes should be approved by relevant business owners and comply with:

a) business continuity plans associated with the business activities supported by the installation
b) legal, regulatory and contractual obligations
c) long-term archiving requirements
d) manufacturer recommendations (eg for storage conditions and maximum 'shelf-life').

CI3.2.4

The security of back-up processes should be strengthened by use of a back-up management package.

CI3.2.5

Back-ups should be:

a) performed in accordance with a defined back-up / archive schedule or cycle that reflects the classification of information being backed up, and ensures that information and systems can be restored within critical timescales
b) performed so that individual files can be recovered
c) related to control points in live processes (eg by using time-stamps)
d) reconciled to the live version when copies are taken (eg by checking of file size, hash totalling or other methods of verification)
e) recorded in a log, or equivalent, and include details such as information backed-up, the date and time of the back-up, and the back-up media used
f) clearly and accurately labelled
g) protected from accidental overwriting, and be subject to the same level of protection as live information
h) verified to ensure backed-up files can be restored successfully
i) retained for at least three generations of the back-up cycle.

(continued on the next page)

Section CI3.2 Back-up (continued)

CI3.2.6

Back-ups should be protected from loss, damage and unauthorised access, by:

a) storing them in readily-accessible locations (eg in a computer media fireproof safe on-site) to enable important information to be restored quickly
b) supporting them with copies kept off-site, to enable required systems to be restored using alternative facilities in case of a disaster
c) restricting access to authorised staff.

CI3.2.7

Data written to back-up media should be encrypted to prevent disclosure of sensitive information to unauthorised individuals.

CI3.2.8

The security of back-ups in transit to and from off-site locations should be assured by use of reputable couriers and protective packaging (eg locked, robust containers).

Section CI3.3 Change management

Principle Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise the security of the installation.

CI3.3.1

A change management process should be established, which covers all types of change (including emergency fixes, changes to business information and upgrades to new versions of software and hardware).

CI3.3.2

The change management process should be documented, and include:

a) approving and testing changes to ensure that they do not compromise security controls
b) performing changes and signing them off to ensure they are made correctly and securely
c) reviewing completed changes to ensure that no unauthorised changes have been made.

CI3.3.3

Prior to changes being applied to the live environment:

a) change requests should be documented (eg on a change request form) and accepted only from authorised individuals
b) changes should be approved by an appropriate business representative
c) the potential business impact of changes should be assessed (eg in terms of overall risk and impact on other components of the installation)
d) change requests should be approved by an appropriate business representative
e) changes should be tested to help determine the expected results of making the change in the live environment
f) changes should be reviewed to ensure that they do not compromise security controls (eg by checking software to ensure it does not contain malware, such as malicious code, a trojan horse or a virus)
g) back-out positions should be established so that the installation can recover from failed changes or unexpected results.

CI3.3.4

Changes to the installation should be:

a) performed by skilled and competent individuals who are capable of making changes correctly and securely
b) supervised by an IT specialist
c) signed off by an appropriate business representative.

CI3.3.5

Arrangements should be made to ensure that once changes have been applied:

a) version control is maintained (eg using configuration management)
b) a record is maintained, showing what was changed, when, and by whom (eg using automated helpdesk / service desk software)
c) details of changes are communicated to relevant individuals (eg associated users, business managers and relevant third parties)
d) checks are performed to confirm that only intended changes have been made (eg by comparing code against a control version)
e) documents associated with the installation are updated (eg design information, system configuration, implementation details, and records of all changes to the installation).

Section CI3.4 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

CI3.4.1

There should be a documented information security incident management process that applies to the installation.

CI3.4.2

The information security incident management process should include:

a) identifying information security incidents
b) responding to information security incidents
c) recovering from information security incidents
d) following up information security incidents.

CI3.4.3

Information security incidents should be:

a) reported to a predetermined contact (eg a helpdesk, telephone hot line or specialist IT team / department)
b) recorded in a log or equivalent (eg using an automated information security incident management system)
c) categorised and classified (eg according to their severity and type).

CI3.4.4

The business impact of serious information security incidents should be assessed by an installation specialist, the owner(s) of application(s) supported by the installation, and an information security specialist.

CI3.4.5

The response to information security incidents should include:

a) analysing available information (eg system event logs)
b) handling necessary evidence (eg labelling it and storing it in a safe location to prevent unauthorised tampering)
c) investigating the cause of information security incidents (eg with assistance from the information security incident management team)
d) containing and eradicating the information security incident (eg by making changes to access control or terminating network connections).

CI3.4.6

The recovery of information security incidents should involve:

a) rebuilding systems (and the applications they support) to a previously known secure state (ie the same state they were in before the information security incident occurred)
b) restoring from information that has not been compromised by the information security incident
c) closure of the information security incident.

(continued on the next page)

Section CI3.4 Information security incident management (continued)

CI3.4.7

Following recovery from information security incidents:

a) reviews should be performed to determine the cause (eg by performing a root cause analysis) and effect of the information security incident and corresponding recovery actions
b) forensic investigations should be performed if required (eg for legal purposes or serious information security incidents, such as fraud)
c) existing security controls should be examined to determine their adequacy
d) corrective actions should be undertaken to minimise risk of similar incidents occurring
e) details of the information security incident should be documented in a post-incident report.

Section CI3.5 Emergency fixes

Principle Emergency fixes to computer equipment, business applications, systems software and business information should be tested, reviewed and applied quickly and effectively, in accordance with documented standards / procedures.

Objective To respond to emergencies in a timely and secure manner, while reducing disruption to the organisation.

CI3.5.1

There should be documented standards / procedures for applying emergency fixes to the computer installation.

CI3.5.2

Standards / procedures should cover:

a) emergency fixes to hardware, business application software, systems software, parameter settings and business and system information within the live environment
b) emergency access for key individuals (eg business owners or users, system administrators, systems development staff and suppliers of equipment, software or services).

CI3.5.3

Emergency fixes should be approved by an appropriate business representative, logged, and carried out in accordance with standards / procedures.

CI3.5.4

Emergency access granted to perform an emergency fix should be revoked as soon as the emergency is over.

CI3.5.5

Once the emergency is over:

a) authorisation for emergency access should be revoked immediately
b) emergency fixes should be documented
c) subject to standard change management disciplines and reviewed by the installation owner
d) emergency fixes should be checked to ensure that they are not left permanently in place.

Section CI3.6 Patch management

Principle A process should be established for managing the application of system and software patches, which is supported by documented standards / procedures.

Objective To address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

CI3.6.1

There should be documented standards / procedures for patch management, which specify the:

a) requirement to patch computer equipment, business applications, operating system / software and network components
b) organisation's approach to patching (eg what is to be patched)
c) testing requirements (eg provision of a test environment)
d) methods of patch distribution (eg automated deployment).

CI3.6.2

Standards / procedures for patch management should include a method of:

a) defining roles and responsibilities for patch management
b) determining the importance of systems (eg based the information handled, the business processes supported and the environments in which they are used)
c) recording patches that have been applied (eg using an inventory of computer assets including their patch level).

CI3.6.3

A patch management process should be established to govern the application of patches on a day-to-day basis. The process should be documented, approved by relevant management, and assigned an owner.

CI3.6.4

The patch management process should:

a) determine methods of obtaining patches
b) specify methods of validating patches (eg ensuring that the patch is from an authorised source)
c) identify vulnerabilities that are applicable to the installation
d) assess the business impact of implementing patches (or not implementing a particular patch)
e) ensure patches are tested against known criteria
f) describe methods of deploying patches (eg using software distribution tools)
g) report on the status of patch deployment within the installation
h) include methods of dealing with the failed deployment of a patch (eg redeployment of the patch).

CI3.6.5

Methods should be established to protect information and systems if no patch is available for an identified vulnerability (eg disabling services and adding additional access controls).

Area CI4
ACCESS CONTROL

Effective access control mechanisms can reduce the risk of unauthorised access to information and systems. Accordingly, this area covers the access control disciplines applied to users and the steps taken to restrict access to information and systems within the computer installation.

Section CI4.1 Access control arrangements

Principle Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation.

Objective To ensure that only authorised individuals gain access to information or systems within the computer installation, and that individual accountability is assured.

CI4.1.1

Arrangements should be made to restrict access to the computer installation, and the information stored and processed in it.

CI4.1.2

Access control arrangements should be supported by documented standards / procedures, which should take account of:

a) an information security policy, information classifications, agreements with application owners, requirements set by the installation owner and legal, regulatory and contractual obligations
b) the need to achieve individual accountability, apply additional control to users with special access privileges and provide segregation of duties.

CI4.1.3

Access control arrangements should cover access:

a) by all types of individual (eg business users, individuals running the installation and IT specialists, such as technical support staff)
b) to all types of information and software (eg live business information, application and system software, access control data, back-up files, and system documentation).

CI4.1.4

Access control arrangements should:

a) restrict access in line with access policies set by application owners
b) restrict the system capabilities that can be accessed (eg by providing menus that enable access only to the particular capabilities needed to fulfil a defined role)
c) identify the location of terminals in use
d) prevent misuse of passwords (eg by using strong authentication, such as smartcards, biometrics or tokens)
e) minimise the need for special access privileges (eg UserIDs that have additional capabilities, such as 'Administrator' in Windows systems, or special capabilities, such as UserIDs that can be used to authorise payments)
f) be reviewed periodically
g) be upgraded in response to new threats, capabilities, business requirements or experience of information security incidents.

Section CI4.2 User authorisation

Principle All users of the computer installation should be authorised before they are granted access privileges.

Objective To restrict access to any information or systems within the computer installation to authorised users.

CI4.2.1

All users of the computer installation should be subject to an authorisation process before they are granted access.

CI4.2.2

The processes for authorising users should:

a) be defined in writing, approved by the installation owner and applied to all users
b) associate access privileges with defined users (eg with UserIDs rather than passwords)
c) issue default access privileges of 'none' (ie rather than 'read')
d) ensure redundant UserIDs are not re-issued for use.

CI4.2.3

A file or database containing details of all authorised users should be established, which should be maintained by designated individuals, such as particular system administrators, and protected against unauthorised change or disclosure.

CI4.2.4

Details of authorised users should be reviewed:

a) to ensure that access privileges remain appropriate
b) to check that redundant authorisations have been deleted (eg for employees who have changed roles or left the organisation)
c) on a regular basis (eg at least every six months)
d) on a more regular basis for users with special access privileges (eg every three months).

Section CI4.3 Access privileges

Principle All users of the computer installation should be assigned specific privileges to allow them to access particular information or systems.

Objective To provide authorised users with access privileges which are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

CI4.3.1

Access privileges for business users and computer staff (eg computer operators and system administrators) should be approved by an appropriate business representative.

CI4.3.2

Before access privileges come into effect:

a) authorisations should be checked to confirm access privileges are appropriate
b) details of users should be recorded (eg their true identity, associated UserIDs and access privileges to be granted)
c) users should be advised of, and be required to confirm understanding of their access privileges and associated conditions.

CI4.3.3

Access privileges should not be assigned collectively (eg UserIDs / passwords shared in a group) unless special circumstances apply. Whenever they need to be assigned collectively, they should be documented, approved by an appropriate business representative and subject to additional controls (eg restricted access privileges and contractual conditions).

CI4.3.4

Additional controls should be applied to special access privileges, including high-level privileges (such as 'root' in UNIX or 'Administrator' in Windows systems), powerful utilities and privileges that can be used to authorise payments. These controls should include:

a) specifying the purpose of special access privileges
b) restricting the use of special access privileges to narrowly defined circumstances
c) requiring individual approval for the use of special access privileges
d) requiring users with special access privileges to sign-on using identification codes or tokens that differ from those used in normal circumstances.

CI4.3.5

A process for terminating the access privileges of users should be established to ensure that:

a) authentication details and access rights are revoked promptly on all systems to which the user had access
b) access profiles / accounts are deleted
c) components dedicated to providing access, such as tokens or modems, are disabled or removed.

Section CI4.4 Sign-on process

Principle Users should follow a rigorous system sign-on process before being provided with access to target systems.

Objective To prevent unauthorised users from gaining access to any information or systems within the computer installation.

CI4.4.1

There should be a sign-on process that users must follow before they can gain access to any systems within the computer installation, which should enable UserIDs to be identified individually.

CI4.4.2

Sign-on mechanisms should be configured so that they:

a) validate sign-on information only when it has all been entered
b) limit the number of unsuccessful sign-on attempts (for example a re-try limit of three)
c) restrict additional sign-on attempts
d) limit the duration of any one sign-on session
e) are reinvoked automatically after interruption (eg following a disconnection from the application).

CI4.4.3

Sign-on mechanisms should be configured to provide information so that they:

a) display no identifying details until after sign-on is completed successfully
b) warn that only authorised users are permitted access
c) record all successful and unsuccessful sign-on attempts
d) advise users (on successful sign-on) of the date / time of their last successful sign-on and all unsuccessful sign-on attempts since their most recent successful sign-on.

CI4.4.4

Sign-on mechanisms should be configured so that they do not store authentication details as clear text in automated routines (eg in scripts, macros or cache memory).

CI4.4.5

The approval of the installation owner should be obtained before any important features of the sign-on process are bypassed, disabled or changed.

Section CI4.5 User authentication

Principle All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (eg smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.

Objective To prevent unauthorised users from gaining access to any information or systems within the computer installation.

CI4.5.1

All users should be authenticated, either by using UserIDs and passwords or by stronger authentication such as smartcards or biometric devices (eg fingerprint recognition) before they can gain access to any information or systems within the installation.

CI4.5.2

Where authentication is achieved by a combination of UserIDs and passwords, users should be advised to keep passwords confidential (ie to avoid writing them down or disclosing them to others) and to change passwords that may have been compromised.

CI4.5.3

User authentication should be enforced by automated means that:

a) ensure UserIDs are unique
b) ensure passwords are not displayed on screen or on print-outs
c) issue temporary passwords to users that must be changed on first use
d) force new passwords to be verified before the change is accepted
e) ensure users set their own passwords
f) ensure passwords are a minimum number of characters in length, differ from their associated UserIDs, contain no more than two identical characters in a row and are not made up of all numeric or alpha characters
g) ensure passwords are changed regularly (eg every 30 days) and more frequently for users with special access privileges
h) restrict the re-use of passwords (eg so that they cannot be used again within a set period or set number of changes).

CI4.5.4

There should be a process for issuing new or changed passwords that:

a) ensures that passwords are not sent in the form of clear text e-mail messages
b) directly involves the person to whom the password uniquely applies
c) verifies the identity of the end user, such as via a special code or through independent confirmation
d) includes notification to users that passwords will expire soon.

CI4.5.5

Strong authentication (eg smartcards or biometric devices, such as fingerprint recognition) should be applied to users with access to critical business applications or sensitive information and to users with special access privileges or access capabilities from external locations.

Area CI5
LOCAL SECURITY MANAGEMENT

A computer installation typically supports one or more critical business applications, holds information that needs to be protected, and is an important asset in its own right. Each of these perspectives needs to be considered in order to provide appropriate protection. Accordingly, this area covers the arrangements made to identify the relative importance of the computer installation, the associated business risks and the level of protection required. It also covers the arrangements made to ensure that information security is co-ordinated locally, staff are aware of information security and understand their personal responsibilities, and the need for the installation to be subject to thorough, independent and regular security audits / reviews.

Section CI5.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate the information security activities associated with the computer installation.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

CI5.1.1

The installation owner should have overall responsibility for information security in relation to the installation. A local information security co-ordinator should be appointed to be responsible for co-ordinating the information security arrangements of the installation and acting as a single point of contact on information security issues.

CI5.1.2

Local information security co-ordinator(s) should have:

a) a sound understanding of their information security roles and responsibilities
b) sufficient skills, time, tools (eg checklists and specialist software products) and authority needed to carry out their assigned role
c) access to in-house or external expertise in information security
d) documented standards / procedures to support day-to-day security activities
e) up-to-date information related to information security on issues (eg users' security requirements, emerging threats and newly discovered vulnerabilities) and techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture)
f) a channel of communication with the information security function.

CI5.1.3

The local information security co-ordinator(s) should meet regularly with the installation owner to review the status of information security in the installation and agree security activities to be performed.

Section CI5.2 Security awareness

Principle Individuals running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure individuals running the installation apply security controls and prevent important information stored in or processed by the installation from being compromised or disclosed to unauthorised individuals.

CI5.2.1

There should be an information security policy that applies to the computer installation. Staff employed in the computer installation should be aware of, and comply with, the information security policy.

CI5.2.2

Individuals employed in the computer installation should:

a) take part in a security awareness programme (eg attend structured awareness training seminars)
b) be provided with information security education / training (eg using techniques such as presentations and computer-based training (CBT))
c) be supplied with specialised security awareness material (eg brochures, reference cards, posters and electronic documents delivered via an organisation's intranet).

Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities.

CI5.2.3

Individuals employed in the computer installation should be made aware of:

a) the meaning of information security (ie the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the installation
c) the importance of complying with information security policies and applying associated standards / procedures
d) their personal responsibilities for information security.

CI5.2.4

Individuals employed in the computer installation should be made aware that they are prohibited from:

a) unauthorised use of any part of the network
b) using the network (or network components) for purposes that are not work-related
c) making sexual, racist or other statements that may be offensive (eg when using e-mail, instant messaging, the Internet, or the telephone)
d) making obscene, discriminatory or harassing statements, which may be illegal (eg when using e-mail, instant messaging, the Internet, or the telephone)
e) downloading illegal material (eg with obscene or discriminatory content)
f) using unauthorised installation components (eg using unauthorised third party software, USB memory sticks or modems)
g) unauthorised copying of information or software
h) disclosing confidential information (eg customer records, product designs or pricing policies) to unauthorised individuals
i) compromising passwords (eg by writing them down or disclosing them to others)
j) using personally identifiable information (ie information that can be used to identify an individual person) unless explicitly authorised
k) tampering with evidence in the case of information security incidents that may require forensic investigation.

(continued on the next page)

Section CI5.2 Security awareness (continued)

CI5.2.5

Individuals should be warned of the dangers of being overheard when discussing business information over the telephone or in public places (eg train carriages, airport lounges or bars).

Section CI5.3 Information classification

Principle Information stored or processed within the computer installation should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to the computer installation, thereby preventing unauthorised disclosure.

CI5.3.1

Information associated with the computer installation should be subject to an information classification scheme (ie a method of classifying information according to its level of confidentiality), which complies with enterprise-wide standards / procedures for information classification.

Some organisations also take into account requirements for integrity (ie the need for information to be valid, accurate and complete) and availability (ie the need for information to be accessible when required) when classifying information.

CI5.3.2

The information classification scheme should:

a) take account of the potential business impact from the loss of confidentiality of information
b) be used to determine varying levels of confidentiality of information (eg top secret, company-in-confidence and public).

CI5.3.3

The information classification scheme should be used to classify information:

a) stored in paper form (eg contracts, plans and system documentation held in hard-copy form)
b) held in electronic form (eg business transactions, financial statistics, product design details and customer files).

Information classification typically involves labelling of:

- information stored in paper form (eg using rubber ink stamps, adhesive labels, hologram lamination)
- information stored in electronic form (eg using electronic watermarking, labelling headers and footers, using filename conventions)
- electronic communications (eg using digital signatures and including the classification in the subject header of e-mails).

CI5.3.4

Information classifications associated with the computer installation should be:

a) signed off by an appropriate business representative
b) reviewed regularly and when changes are made to the application.

CI5.3.5

Information classification details associated with the computer installation should be recorded in:

a) an inventory, or equivalent (eg a database, specialised piece of software, or on paper)
b) agreements with service providers.

(continued on the next page)

Section CI5.3 Information classification (continued)

CI5.3.6

Information classification details should include:

a) the classification of the information (eg top secret, company-in-confidence and public)
b) the identity of the information owner
c) a brief description of the information classified.

Section CI5.4 Information risk analysis

Principle The computer installation should be subject to an information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed.

Objective To identify key information risks associated with the computer installation and determine the security controls required in order to keep those risks within acceptable limits.

CI5.4.1

The computer installation should be subject to an information risk analysis, performed in compliance with enterprise-wide standards / procedures for information risk analysis, using a structured information risk analysis methodology.

Information risk analysis (sometimes referred to as simply risk analysis or risk assessment) is the identification, measurement and prioritisation of risk, and the selection of security controls to mitigate that risk. An example of a structured methodology is the ISF's Information Risk Analysis Methodology (IRAM).

CI5.4.2

The information risk analysis should take into consideration critical business applications supported by the installation and associated service level agreements (SLAs).

CI5.4.3

The information risk analysis should involve:

a) business owners of critical business applications supported by the installation
b) the installation owner
c) an IT specialist
d) key user representatives
e) an expert in risk analysis (eg a member of staff or a third party specialist who has appropriate experience as an information risk analysis practitioner)
f) an information security specialist (eg a member of staff or a third party specialist who has appropriate experience as an information security practitioner).

CI5.4.4

The information risk analysis should determine risk by assessing:

a) the potential level of business impact associated with the installation
b) accidental and deliberate threats to the confidentiality, integrity or availability of information (eg denial of service attacks, malware, misusing systems to commit fraud, loss of power, malfunctions and human error) stored in or processed by the installation
c) vulnerabilities due to control weaknesses
d) vulnerabilities due to circumstances that increase the likelihood of a serious information security incident occurring (eg use of the Internet, permitting third party access or siting a computer installation in an area prone to earthquakes or flooding).

(continued on the next page)

Section CI5.4 Information risk analysis (continued)

CI5.4.5

The information risk analysis should take into account:

a) compliance requirements (eg legislation, regulation, industry standards and internal policies)
b) objectives of the organisation
c) information classification requirements
d) previous risk analyses conducted on the computer installation being assessed
e) characteristics of the operating environment of the application, network or computer installation being assessed.

CI5.4.6

Results of the information risk analysis should be documented and should include:

a) a clear identification of key risks
b) an assessment of the potential business impact of each risk
c) recommendations for the actions required to reduce risk to an acceptable level.

CI5.4.7

The information risk analysis should be used to help:

a) select information security controls that will reduce the likelihood of serious information security incidents occurring
b) select information security controls that will satisfy relevant compliance requirements (eg the Sarbanes-Oxley Act 2002, the Payment Card Industry (PCI) Data Security Standard, Basel II 1998, data privacy requirements and anti-money laundering laws)
c) determine the costs of implementing security controls (eg costs associated with: design, purchase, implementation and monitoring of the controls; hardware and software; training; overheads, such as facilities; and consultancy fees)
d) evaluate the strengths and weaknesses of security controls
e) identify specialised security controls required by the installation (eg encryption or strong authentication).

CI5.4.8

Results of the information risk analysis (including risk treatment actions and any identified residual risk) should be:

a) communicated to the installation owner and top management (eg board-level executives or equivalent)
b) signed off by an appropriate business representative.

Risk treatment typically involves one of four options: applying appropriate controls; accepting risks; avoiding risks; or transferring risks. Residual risk is that proportion of risk that still remains after selected controls have been implemented.

CI5.4.9

Information risk analyses of the installation should be performed regularly and before major changes to the installation are implemented.

Section CI5.5 Security audit / review

Principle The information security status of the computer installation should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls have been implemented effectively, that risk is being managed and to provide the installation owner, and top management, with an independent assessment of the security status of the installation.

CI5.5.1

Security audits / reviews of the computer installation should be performed regularly and carried out independently of individuals running or supporting the installation (eg by a third party specialist or by internal audit).

CI5.5.2

Security audits / reviews should:

a) assess the business risks associated with the installation
b) consider the information security requirements of the business applications supported by the installation.

CI5.5.3

Security audits / reviews of the installation should assess the status of information security arrangements in key areas (eg installation management, the live environment, system operation, access control, local security management and business continuity).

CI5.5.4

Security audits / reviews of the installation should be:

a) agreed with the installation owner
b) defined in scope, and documented
c) performed by experienced and qualified individuals who have sufficient technical skills and knowledge of information security
d) conducted frequently and thoroughly (in terms of scope and extent) to provide assurance that security controls function as required
e) focused on ensuring that controls are effective enough to reduce risks to acceptable levels
f) supplemented by the use of automated software tools
g) validated by competent individuals
h) complemented by reviews carried out by independent third parties.

(continued on the next page)

Section CI5.5 Security audit / review (continued)

CI5.5.5

Security audit / review activity should be managed by:

a) agreeing requirements for special processing routines or tests (eg network, system and application penetration testing) with the installation owner
b) restricting access to the installation by the audit / review team (eg by granting only 'read' access to business information and software files or other types of access only for isolated copies of business information and software files)
c) monitoring and logging the activities of the audit / review team
d) disposing of business information copied for the purpose of an audit / review as soon as it is no longer required protecting software tools used in carrying out audits / reviews (eg by keeping them separate from tools / utilities used in the live environment and holding them in secure storage facilities, such as restricted software libraries)
e) protecting documents and system files relating to the audit / review.

CI5.5.6

Recommendations following security audits / reviews should be agreed with the installation owner, and reported to top management (eg board-level executives or equivalent).

Area CI6
SERVICE CONTINUITY

If there is a serious interruption to information processing, (eg if a disaster occurs), the computer installation may be unavailable for a prolonged period. Considerable forethought is required to enable information processing to continue in these circumstances and to keep the business impact to a minimum. Accordingly, this area covers the development of contingency plans and arrangements, and their validation.

Section CI6.1 Contingency plans

Principle A contingency plan should be developed and documented.

Objective To provide individuals with a documented set of actions to perform in the event of a disaster, enabling information processing to be resumed within critical timescales.

CI6.1.1

There should be a contingency plan that covers the computer installation, the format and content of which should comply with enterprise-wide standards / procedures for contingency planning.

CI6.1.2

The contingency plan should form part of a wider business continuity plan and be distributed to all individuals who would require it in case of an emergency. Such individuals should be informed of their responsibilities and provided with relevant training / tools to fulfil them.

CI6.1.3

The contingency plan should be developed in conjunction with user representatives. It should be based on a set of scenarios of possible disasters and identification of the key business processes to be protected by the plan.

CI6.1.4

The contingency plan should specify:

a) conditions for its invocation
b) the critical timescales associated with the business applications supported by the installation
c) a schedule of key tasks to be carried out
d) procedures in sufficient detail so that they can be followed by individuals who do not normally carry them out
e) information security controls applied during the recovery process.

CI6.1.5

The contingency plan should include:

a) responsibilities for carrying out tasks and activities, including deputies
b) procedures to be followed in completing key tasks and activities, including emergency, fall-back and resumption procedures
c) procedures to be followed by business users.

(continued on the next page)

Section CI6.1 Contingency plans (continued)

CI6.1.6

The contingency plan should include arrangements for:

a) processing from last successful back-up to time of disaster and then to resumption of normal service
b) resuming processing using alternative facilities (eg via reciprocal arrangements with another organisation or a contract with a specialist business continuity arrangements provider).

CI6.1.7

Custody of the contingency plan should be the responsibility of a specific individual or working group and copies of the plan should be stored securely off-site.

Section CI6.2 Contingency arrangements

Principle Alternative processing arrangements should be established, and made available when required.

Objective To enable information processing to resume within critical timescales, using alternative facilities.

CI6.2.1

Alternative information processing arrangements should be established to enable services to continue in the event of a disaster affecting the computer installation (eg alternative computer facilities within the organisation or at a third party site).

CI6.2.2

Contingency arrangements should be made to enable the computer installation to continue processing information in the event of prolonged unavailability of:

a) key individuals (eg due to illness, injury, vacation or travel)
b) system or application software
c) critical information (eg business information, documentation, back-up files in paper or electronic form)
d) access to systems or buildings (eg due to police, military or terrorist action, natural disaster, or withdrawal of transport services)
e) essential services (eg loss of utilities such as electricity, gas or water supplies)
f) telephone lines
g) important computer, communications and environmental control equipment
h) system documentation (including operating procedures and parameter settings).

CI6.2.3

Contingency arrangements should cover all locations supported by the installation and all business users who are able to access systems within the installation.

Section CI6.3 Validation and maintenance

Principle Contingency plans and arrangements should be tested on a regular basis.

Objective To ensure that information processing can resume within critical timescales, using alternative facilities.

CI6.3.1

Contingency plans and arrangements for the installation should be tested regularly, and at least annually.

CI6.3.2

Tests of contingency plans and arrangements should:

a) include realistic simulations, involving both business users and IT staff
b) demonstrate that processing can resume within critical timescales.

CI6.3.3

The updating of contingency plans and arrangements should be:

a) the responsibility of a designated individual or working group
b) performed following significant changes to business processes
c) revised in response to problems encountered during tests / rehearsals.

CI6.3.4

The need for changes to contingency plans and arrangements should be considered regularly (eg at least monthly).

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

Networks

Computer networks convey information and provide a channel of access to information systems. By their nature, they are highly vulnerable to disruption and abuse. Safeguarding business communications requires robust network design, well-defined network services, and sound disciplines to be observed in running networks and managing security. These factors apply equally to local and wide area networks, and to data and voice communications.

Networks

NW1 Network Management

NW1.1 Roles and responsibilities

NW1.2 Network design

NW1.3 Network resilience

NW1.4 Network documentation

NW1.5 Service providers

NW2 Traffic Management

NW2.1 Configuring network devices

NW2.2 Firewalls

NW2.3 External access

NW2.4 Wireless access

NW3 Network Operations

NW3.1 Network monitoring

NW3.2 Change management

NW3.3 Information security incident management

NW3.4 Physical security

NW3.5 Back-up

NW3.6 Service continuity

NW3.7 Remote maintenance

NW4 Local Security Management

NW4.1 Local security co-ordination

NW4.2 Security awareness

NW4.3 Information classification

NW4.4 Information risk analysis

NW4.5 Security audit / review

NW5 Voice Networks

NW5.1 Voice network documentation

NW5.2 Resilience of voice networks

NW5.3 Special voice network controls

NW5.4 Voice over IP (VoIP) networks

Area NW1
NETWORK MANAGEMENT

Computer networks are complex. They have to link different systems together, are subject to constant change and often rely on services provided by external parties. Orchestrating the technical and organisational issues involved requires sound management. Accordingly, this area covers the organisational arrangements for running a network, its design, resilience and documentation, and the management of relationships with service providers.

Section NW1.1 Roles and responsibilities

Principle An owner should be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To achieve individual accountability for the network, provide a sound management structure for staff running the network and give responsible individuals a vested interest in its protection.

NW1.1.1

An owner should be appointed for managing the network. Responsibilities for key network management tasks should be clearly assigned to one or more capable individuals, who should accept the responsibilities (including those for information security) associated with these roles.

NW1.1.2

Network staff should be:

a) competent to run the network under normal conditions
b) able to deal with error, exception and emergency conditions
c) sufficient in number to handle normal and peak workloads.

NW1.1.3

The risk of staff disrupting the running of the network either in error or by malicious intent should be reduced by:

a) separating the duties of staff running the network from the duties of staff designing and developing the network
b) ensuring internal staff (eg network operations and administrators) and external individuals (eg consultants, contractors, engineers) sign non-disclosure / confidentiality agreements
c) minimising reliance on key individuals (eg by automating processes, ensuring supporting documentation is complete and accurate, and arranging alternative cover for key positions)
d) organising duties in such a way as to minimise the risk of theft, fraud, error and unauthorised changes to information (eg by supervising and recording activities, prohibiting lone working and the segregation of duties)
e) screening applicants for positions that involve running the network (eg by taking up references, checking career history / qualifications and confirming identity by inspecting a passport).

(continued on the next page)

Section NW1.1 Roles and responsibilities (continued)

NW1.1.4

There should be documented standards / procedures that apply to the network, which are:

a) consistent with information security policies that apply enterprise-wide
b) communicated to internal and external individuals involved in running the network
c) approved by an appropriate business representative, reviewed regularly and kept-up-to-date.

NW1.1.5

The activities of individuals running the network should be monitored (eg by providing supervision, recording activities and maintaining audit trails).

Section NW1.2 Network design

Principle The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.

Objective To produce an operational network that has security functionality built-in and enables additional controls to be incorporated easily.

NW1.2.1

The design of the network should be supported by documented standards / procedures, which require the:

a) design to take account of users' service requirements (eg as defined in service level agreements)
b) network to be compatible with other networks used by the organisation
c) network to be configured to cope with foreseeable developments in the organisation's use of IT.

NW1.2.2

The design of the network should:

a) incorporate a coherent, integrated set of technical standards
b) support consistent naming conventions (eg when assigning IP addresses)
c) incorporate the use of security domains (including Demilitarised Zones (DMZs)) to segregate systems with specific security requirements
d) employ firewalls in a manner that prevents them from being bypassed
e) minimise single points of failure (eg by providing load balancing, duplicate or alternative critical network devices)
f) restrict the number of entry points into the network
g) allow end-to-end network management from a primary location
h) enable the network to be remotely configured, and automatically monitored against predefined thresholds
i) enable network management reports and audit trails to be maintained
j) comply with statutory and industry regulations
k) prevent unauthorised devices from connecting to the network (eg by forcing authentication at the network level)
l) include encryption of administrative access to network devices (eg firewalls and intrusion detection sensors).

Section NW1.3 Network resilience

Principle The network should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective To ensure that the network is available when required.

NW1.3.1

Network facilities that are critical to the functioning of the network should be identified.

NW1.3.2

Single points of failure should be minimised by:

a) re-routing network traffic automatically when critical nodes or links fail
b) providing alternative locations from which the network can be administered
c) installing duplicate or alternative firewalls, network traffic filters, main switching nodes, and power supplies to critical communications equipment
d) arranging fall-back to alternative points of connection and links with external service providers.

NW1.3.3

The risk of malfunction of critical communications equipment, software, links and services should be reduced by:

a) giving high priority to reliability, compatibility (eg with other networks controlled by the organisation) and capacity (eg bandwidth) in the acquisition process
b) ensuring compliance with common or industry standards
c) using only proven and up-to-date equipment, software, links and services
d) maintaining consistent versions of network equipment and software across the network
e) ensuring that key network components can be replaced within critical timescales.

NW1.3.4

The availability of external network services should be protected by:

a) providing duplicate or alternative points of connection to external communications carriers
b) routing critical links to more than one external exchange or switching centre
c) arranging for use of an alternative communications carrier.

NW1.3.5

There should be a process for dealing with vulnerabilities in firewalls, which include:

a) monitoring vulnerabilities in firewalls (eg by running firewall checking software, and tracking CERT alerts, vendor websites and mailing lists)
b) issuing instructions to network staff on the action to be taken if a firewall fails
c) automatically re-routing network traffic to an alternative firewall
d) testing patches for firewalls and applying them in a timely manner.

Section NW1.4 Network documentation

Principle Networks should be supported by accurate, up-to-date documentation.

Objective To ensure that the network is configured accurately and securely.

NW1.4.1

The network should be supported by documented standards / procedures, which cover the documentation of:

a) the configuration of the network, including all nodes and connections
b) communications equipment, software, links and services
c) in-house cabling.

NW1.4.2

Network documentation should include:

a) network configuration diagrams, showing nodes and connections
b) an inventory of communications equipment, software and services provided by external parties
c) one or more diagrams of in-house cable runs.

NW1.4.3

Network documentation (eg diagrams, inventories and schedules) should be:

a) kept up-to-date
b) readily accessible to authorised individuals
c) subject to supervisory review
d) generated automatically, using software tools.

NW1.4.4

Identification labels should be attached to communications equipment and cables.

Section NW1.5 Service providers

Principle Network services should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.

Objective To define the business requirements for network service providers, including those for security, and ensure they are met.

NW1.5.1

Documented agreements (eg contracts or service level agreements) should be established with all internal and external service providers.

A service level agreement (SLA) should include all key elements, such as: who is in charge of the application (ie the application owner); who is in charge of delivering the required service (eg an internal or external service provider); capacity requirements; maximum permissible down-time; and criteria for measuring the level of service.

NW1.5.2

Agreements with service providers should specify:

a) individuals responsible for the service within both parties to the agreement
b) capacity requirements, dates / times when network services are required and critical timescales of the network
c) restrictions on methods of connection (eg broadband, ISDN or dial-up) and access to particular services (eg public Internet services).

NW1.5.3

Agreements with service providers should specify requirements for:

a) ensuring continuity of service
b) patching of network devices
c) protecting confidential information in transit (eg by using encryption)
d) segregating network components, such as dedicated lines for sensitive network traffic
e) performing change management and information security incident management
f) detecting service interruptions and recovering from them
g) installation and maintenance activity relating to the network.

NW1.5.4

The conditions of agreements with service providers should be enforced, and reviewed regularly.

NW1.5.5

Arrangements should be made with service provider(s) to deal with information security issues via a defined point of contact and through an individual who is sufficiently senior and competent to deal with security issues effectively.

NW1.5.6

Arrangements should be made to:

a) restrict the use of services to approved network providers
b) obtain independent confirmation of security controls applied by the service providers.

Area NW2
TRAFFIC MANAGEMENT

Computer networks can handle many types of traffic from a wide variety of sources. To manage network traffic effectively, network devices (eg firewalls) have to be configured correctly and particular types of network traffic denied access. Accordingly, this area covers the disciplines required to ensure undesirable network traffic and unauthorised external or wireless users are prevented from gaining access to the network.

Section NW2.1 Configuring network devices

Principle Network devices (eg routers, switches and firewalls) should be configured to function as required, and to prevent unauthorised or incorrect updates.

Objective To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

NW2.1.1

There should be documented standards / procedures for configuring network devices (eg routers, hubs, bridges, concentrators, switches and firewalls), which cover:

a) managing changes to routing tables and settings in network devices
b) restricting access to network devices
c) preventing unauthorised or incorrect updates to routing tables
d) regular review of network device configuration.

NW2.1.2

Network devices should be configured to:

a) deny network traffic by default, and fail secure
b) highlight overload or exception conditions when they occur
c) log events in a form suitable for review, and record them on a separate system
d) copy control information (eg event logs and tables) to removable storage media (eg CD or magnetic tape)
e) integrate with access control mechanisms in other devices (eg to provide strong authentication)
f) use a predefined secure set-up upon boot
g) change vendor-supplied default parameters (eg passwords and SNMP community strings)
h) ensure that passwords are not sent in clear text form
i) disable source routing (to retain control within the packet-forwarding device)
j) disable services that are not required for the standard operation of the network (eg RPC, rlogin, rsh, rexec and NetBIOS).

NW2.1.3

Network devices should be restricted to authorised network staff using access controls that support individual accountability, and be protected from unauthorised access.

(continued on the next page)

Section NW2.1 Configuring network devices (continued)

NW2.1.4

Routers (including network devices that perform routing) should be configured to prevent unauthorised or incorrect updates by:

a) verifying the source of routing updates (eg by using techniques such as Open Shortest Path First (OSPF) or Routed Internet Protocol (RIP))
b) verifying the destination of routing updates (eg by transmitting updates only to specific routers)
c) protecting the exchange of routing information (eg by using passwords)
d) encrypting the routing information being exchanged.

NW2.1.5

Network devices should be reviewed regularly to verify configuration settings (eg routing tables and parameters) and assess activities performed through the network device (eg by inspecting logs).

Section NW2.2 Firewalls

Principle Network traffic should be routed through a well-configured firewall, prior to being allowed access to the network, or before leaving the network.

Objective To prevent unauthorised network traffic from gaining access to the network, or leaving the network.

NW2.2.1

The network should be protected from other networks or sub-networks (internal or external) by one or more firewalls.

NW2.2.2

There should be documented standards / procedures for managing firewalls, which cover:

a) filtering of specific types or sources of network traffic (eg IP addresses, TCP ports or information about the state of communications and users)
b) blocking or otherwise restricting particular types or sources of network traffic
c) the development of predefined rules (or tables) for filtering network traffic
d) protecting firewalls against attack or failure (eg by restricting access to authorised individuals)
e) limiting the disclosure of information about the network.

NW2.2.3

Firewalls should be used to check:

a) destination addresses (eg IP addresses) and ports (eg TCP ports)
b) information about the state of associated communications (eg saving the outgoing port command of an FTP session so that an associated, incoming FTP communication can be checked against it)
c) information about the state of users (eg permitting access to users only where they have been authenticated in a previous communication)
d) the validity of a network service (eg by using an application proxy firewall).

NW2.2.4

Firewalls should be configured to:

a) deny network traffic by default, and fail secure
b) protect communication protocols that are prone to abuse (eg DNS, FTP, NNTP, RIP, SMTP, Telnet, UUCP)
c) block network packets typically used to execute 'denial of service' attacks (eg ICMP Echo, UDP and TCP Echo, Chargen and Discard)
d) deny incoming traffic where the source address is known to have been 'spoofed' (eg where the source address belongs to the network but originates from outside it)
e) deny outgoing traffic where the source address is known to have been 'spoofed' (eg where the source address does not belong to the network but originates from inside it).

NW2.2.5

Firewalls should be configured to block or otherwise restrict communications based on specified source / destination:

a) addresses (eg a particular IP address)
b) ports (eg ports 20 and 21 for FTP, port 23 for Telnet).

(continued on the next page)

Section NW2.2 Firewalls (continued)

NW2.2.6

Filtering of network traffic should be based on predefined rules (or tables) that:

a) have been developed by trusted individuals, and are subjected to supervisory review
b) are based on the principle of 'least access'
c) are documented and kept up-to-date
d) take account of an information security policy, network standards / procedures and user requirements.

NW2.2.7

Before new or changed rules are applied to firewalls, their strength and correctness should be verified, and they should be signed off by the network owner.

NW2.2.8

Disclosure of information about the network should be limited at the:

a) network level by using network address translation (NAT) (eg by replacing internal addresses when exiting the network)
b) application level by using port address translation (PAT) (eg by passing HTTP requests through a HTTP proxy server).

Section NW2.3 External access

Principle All external connections to the network should be individually identified, verified, recorded, and approved by the network owner.

Objective To prevent unauthorised external users from gaining access to the network.

NW2.3.1

There should be documented standards / procedures for controlling external access to the network, which specify that:

a) external connections should be identified
b) the network should be configured to restrict access
c) only authorised types of remote access connection devices are permitted
d) details of external connections should be documented
e) external connections should be removed when no longer required.

NW2.3.2

External connections should be individually identified, and approved by the network owner.

NW2.3.3

A record of external connections should be maintained (eg in an inventory or equivalent), which includes:

a) details of authorised external individuals
b) areas of the IT infrastructure accessible to external users (eg application or network domains).

NW2.3.4

The network should be designed to:

a) conceal network names and topologies from external parties, (eg by using dual or split network directories / name servers)
b) restrict external network traffic to only specified parts of the network
c) restrict connections to defined entry points (eg specific network gateways)
d) verify the source of external connections (eg by using Calling Line Identification (CLI)).

NW2.3.5

Unauthorised external connections should be identified (eg for investigation and possible removal) by:

a) performing manual audits of network equipment and documentation to identify discrepancies with records of known external connections
b) employing network management and diagnostic tools (eg port probes and network discovery / mapping tools)
c) checking accounting records of bills paid to telecommunications suppliers and reconciling them against known connections.

NW2.3.6

Dial-up connections should be protected by using dial-back security (to verify the source of dial-up connection), which is implemented by:

a) configuring mandatory dial-back for all accounts authorised to connect through an access point
b) disconnecting the line at the host, rather than at the client
c) disabling call-forwarding for the dial-back line.

(continued on the next page)

Section NW2.3 External access (continued)

NW2.3.7

External access should be provided using a dedicated remote access server, which:

a) provides reliable and complete authentication for external connections (eg by running an authentication system such as Radius or TACACS+)
b) provides information for troubleshooting (eg modem status and history data)
c) logs all connections and sessions, including details of call start / stop time, call duration and user tracking
d) helps identify possible information security breaches (eg by logging all events in a database and collating them centrally).

NW2.3.8

External connections should be removed promptly when no longer required and any dedicated components disabled or removed (eg redundant modems, communication lines, pre-allocated telephone numbers or network connection cards).

Section NW2.4 Wireless access

Principle Wireless access should be authorised, users authenticated, and wireless traffic encrypted.

Objective To ensure that only authorised individuals gain wireless access to the network and minimise the risk of wireless transmissions being monitored, intercepted or modified.

NW2.4.1

Wireless access to the network should be subject to an information risk analysis and signed off by the network owner, prior to its implementation.

NW2.4.2

There should be documented standards / procedures for controlling wireless access to the network, which cover:

a) placement and configuration of wireless access points (hardware devices that provide interfaces between the wireless network and a wired network)
b) methods of limiting access to authorised users
c) use of encryption (eg WEP, WPA, WPA2) for protecting information in transit
d) detection of unauthorised wireless access points and wireless devices (eg by roaming buildings with a wireless network detector).

NW2.4.3

Wireless access points should be:

a) configured for low power to limit range
b) placed in locations that minimise the risk of interference (eg radio transmitters, microwave ovens and cordless telephones)
c) configured and managed from a central location
d) assigned a unique Service Set Identifier (SSID).

NW2.4.4

The network should be protected against unauthorised wireless access by using a security 'filtering' device (eg a firewall or edge server).

NW2.4.5

Wireless access should be protected by the use of:

a) network access control (eg IEEE 802.1X)
b) device authentication (eg EAP-TLS)
c) user authentication.

NW2.4.6

Wireless access should be protected by:

a) using encryption (eg WEP, WPA and WPA2) between computing devices and wireless access points
b) changing encryption keys regularly.

NW2.4.7

Critical wireless access connections should be subject to additional security controls, such as virtual private networks (VPNs).

Area NW3
NETWORK OPERATIONS

Maintaining continuity of service to users requires computer networks to be run in accordance with sound disciplines. Accordingly this area covers the arrangements needed to monitor network performance and to manage changes and information security incidents. In addition, the area covers the arrangements required to provide physical security, perform back-ups and ensure service continuity.

Section NW3.1 Network monitoring

Principle Network activity should be monitored using a range of techniques such as capacity planning; review of network and intrusion detection logs; and examination of usage reports from service providers.

Objective To assess the performance of the network, reduce the likelihood of network overload and detect potential or actual malicious intrusions.

NW3.1.1

The performance of the network should be monitored:

a) against agreed targets (eg as defined in a service level agreement)
b) by reviewing current utilisation of network facilities at normal and peak periods
c) using automated network monitoring software
d) by reviewing logs of network activity regularly
e) by investigating bottlenecks / overloads.

NW3.1.2

Capacity planning activities should be undertaken to allow extra network capacity to be commissioned before projected bottlenecks / overloads occur.

NW3.1.3

Monitoring activities should be conducted on a regular basis, which involve:

a) scanning host systems and network devices accessible via the network for known vulnerabilities, such as by using specialised products (eg Nessus, Pingware or SATAN)
b) checking whether powerful and unnecessary utilities / commands have been disabled on network devices (eg by using a 'sniffer')
c) checking for the existence and configuration of unauthorised wireless networks (eg by using third party products such as Netstumbler, KISMET and Airsnort)
d) discovering the existence of unauthorised systems (eg by using network discovery and mapping tools).

(continued on the next page)

Section NW3.1 Network monitoring (continued)

NW3.1.4

Intrusion detection mechanisms should be employed that include:

a) detection of known attack characteristics (eg denial of service or buffer overflows)
b) a process for performing regular updates to intrusion detection software, to incorporate new or updated attack characteristics
c) provision of alerts when suspicious activity is detected, supported by documented processes for responding to suspected intrusions (eg information security incident management)
d) protection of intrusion detection mechanisms against attack (eg by preventing the transmission of any outbound network traffic, or by using a network tap to hide the presence of sensors).

NW3.1.5

The use of network analysis / monitoring tools should be restricted to authorised individuals.

NW3.1.6

Usage reports from service providers (eg invoices) should be examined to discover any unusual use of the network or network facilities.

NW3.1.7

The results of monitoring activities should be reviewed by the network owner and presented to the application and installation owners to whom services are provided.

Section NW3.2 Change management

Principle Changes to the network should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise the security of the network.

NW3.2.1

A change management process should be established, which covers all types of change to the network (eg upgrades to communications equipment and software, introduction of new services from service providers and temporary or emergency fixes to the network).

NW3.2.2

The change management process should be documented, and include:

a) approving and testing changes to ensure that they do not compromise security controls
b) performing changes and signing them off to ensure they are made correctly and securely
c) reviewing completed changes to ensure that no unauthorised changes have been made.

NW3.2.3

Prior to changes being applied to the live environment (ie the network):

a) change requests should be documented (eg on a change request form) and accepted only from authorised individuals
b) changes should be approved by an appropriate business representative
c) the potential business impact of changes should be assessed (eg in terms of overall risk and impact on other components of the network)
d) changes should be tested
e) changes should be reviewed to ensure that they do not compromise security controls (eg by checking software to ensure it does not contain malware)
f) back-out positions should be established so that the network can recover from failed changes or unexpected results.

NW3.2.4

Changes to the network should be:

a) performed by skilled and competent individuals who are capable of making changes correctly and securely
b) supervised by a network specialist
c) signed off by an appropriate business representative.

NW3.2.5

Arrangements should be made to ensure that once changes have been applied:

a) version control is maintained (eg using configuration management)
b) a record is maintained, showing what was changed, when, and by whom (eg using automated helpdesk / service desk software)
c) details of changes are communicated to relevant individuals (eg associated users, business managers and relevant third parties)
d) checks are performed to confirm that only intended changes have been made (eg by comparing code against a control version)
e) documents associated with the network are updated (eg design information, system configuration, implementation details, and records of all changes to the network)
f) a security audit / review of the network is performed.

Section NW3.3 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve network information security incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

NW3.3.1

There should be a documented information security incident management process that applies to the network.

NW3.3.2

The information security incident management process should include:

a) identifying information security incidents
b) responding to information security incidents
c) recovering from information security incidents
d) following up information security incidents.

NW3.3.3

Network-related information security incidents should be:

a) reported to a predetermined contact (eg a helpdesk, telephone hotline or specialist IT team / department)
b) recorded in a log or equivalent (eg using an automated information security incident management system)
c) categorised and classified (eg according to their severity and type).

NW3.3.4

The business impact of serious network-related information security incidents should be assessed by a network specialist, the network owner, owners of the applications supported by the network and an information security specialist.

NW3.3.5

The response to network-related information security incidents should include:

a) analysing available information (eg network device event logs)
b) handling necessary evidence (eg labelling it and storing it in a safe location to prevent unauthorised tampering)
c) investigating the cause of the information security incident (eg with assistance from the information security incident management team)
d) containing and eradicating the information security incident (eg by making changes to access control or terminating network connections).

NW3.3.6

The recovery of network-related information security incidents should involve:

a) rebuilding networks (and supporting IT facilities) to a previously known secure state (ie the same state they were in before the information security incident occurred)
b) restoring from information that has not been compromised by the information security incident
c) closure of the information security incident.

(continued on the next page)

Section NW3.3 Information security incident management (continued)

NW3.3.7

Following recovery from network-related information security incidents:

a) reviews should be performed to determine the cause (eg by performing a root cause analysis) and effect of the information security incident and corresponding recovery actions
b) forensic investigations should be performed if required (eg for legal purposes or serious information security incidents, such as fraud)
c) existing security controls should be examined to determine their adequacy
d) corrective actions should be undertaken to minimise risk of similar incidents occurring
e) details of the information security incident should be documented in a post-incident report.

Section NW3.4 Physical security

Principle Physical access to critical network facilities should be restricted to authorised individuals.

Objective To prevent services being disrupted by loss of, or damage to, communications equipment, power or facilities.

NW3.4.1

Physical access to critical network areas (eg network operations centres, equipment rooms, firewalls) should be restricted to authorised individuals. External individuals (eg consultants, contractors, engineers) should be supervised when they have access to communications equipment.

NW3.4.2

Critical network areas (eg network operation centres or rooms housing important network equipment, including those at remote sites) should be protected from:

a) natural hazards (eg fire and flood)
b) power failure (eg by the use of uninterruptible power supplies (UPSs) and batteries)
c) intruders (eg by fitting locks on doors and shutters on windows).

NW3.4.3

Communications cables should be protected by:

a) concealed installation
b) armoured conduit
c) locked inspection / termination points
d) alternative feeds or routing
e) avoidance of routes through publicly accessible areas.

NW3.4.4

Network access points should be protected by:

a) locating them in secure environments (eg locked rooms)
b) disabling them on the network device (eg a network switch) until required.

Section NW3.5 Back-up

Principle Back-ups of essential information and software used by the network should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential network information or software required by the network can be restored within critical timescales.

NW3.5.1

Back-ups of essential information and software (eg business information, systems information and application information) should be performed frequently enough to meet business requirements.

NW3.5.2

Back-ups should be:

a) performed using a back-up management package to strengthen the security of backed-up information
b) encrypted to protect important information (eg in the event back-up media is stolen or is lost in transit to an alternative location, such as an off-site storage facility)
c) recorded in a log (or equivalent), which includes details about backed-up data, the date and time of the back-up, and the back-up media used
d) verified to ensure that backed-up software and information can be restored successfully.

NW3.5.3

Back-up arrangements should enable the network to be restored within critical timescales (ie the point in time beyond which unacceptable loss would be suffered).

NW3.5.4

Back-ups should be protected from loss, damage and unauthorised access, by:

a) storing them in a computer media fireproof safe on-site, to enable important information to be restored quickly
b) supporting them by copies kept off-site, in case of a disaster
c) restricting access to authorised individuals.

Section NW3.6 Service continuity

Principle A service continuity plan should be established, supported by effective contingency arrangements, and tested regularly.

Objective To enable critical network services to continue in the event of a disaster.

NW3.6.1

Checks should be carried out to ensure that continuity of network services is included in IT / network contingency plans (or equivalent), and business continuity plans associated with the business activities supported by the network.

NW3.6.2

Arrangements should be made to enable critical network services to continue in the event of a prolonged unavailability of:

a) the network operations centre(s)
b) critical network equipment
c) network links on company premises (eg in-house cable runs)
d) communications software, control data, and documentation
e) network staff
f) buildings, equipment rooms, power and other vital services.

NW3.6.3

Service continuity arrangements should be:

a) documented
b) reviewed by user representatives
c) approved by the network owner
d) subject to a change management process
e) tested on a regular basis, using realistic simulations, and involving network staff
f) updated following significant changes (such as to network services / facilities or legal, regulatory or contractual obligations).

NW3.6.4

Back-up generators should be:

a) available to handle an extended loss of power to critical communications equipment
b) tested regularly.

Section NW3.7 Remote maintenance

Principle Remote maintenance of the network should be restricted to authorised individuals, confined to individual sessions, and subject to review.

Objective To prevent unauthorised access to the network through the misuse of remote maintenance facilities.

NW3.7.1

Access to the network by external individuals for remote maintenance purposes (eg remote diagnosis / testing, software maintenance) should be managed by:

a) defining and agreeing the objectives and scope of planned work
b) authorising sessions individually
c) restricting access rights so that they do not exceed those required to meet the objectives and scope of planned work
d) logging all activity undertaken
e) revoking access rights and changing passwords immediately after agreed maintenance is complete
f) performing an independent review of remote maintenance activity.

NW3.7.2

Diagnostic ports on network equipment should be protected by access controls (eg passwords and physical locks).

Area NW4
LOCAL SECURITY MANAGEMENT

Computer networks play an essential role in the functioning of many critical business applications. They convey information that needs to be protected, and are valuable assets in their own right. Accordingly, this area covers the arrangements made to identify the relative importance of the network, the associated business risks and the level of protection required. The area also covers the arrangements made to ensure that information security is co-ordinated locally, network staff are aware of information security and understand their personal responsibilities, and the need for the network to be subject to thorough, independent and regular security audits / reviews.

Section NW4.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate the information security activities associated with the network.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

NW4.1.1

The network owner should have overall responsibility for information security in relation to the network. One or more local information security co-ordinators should be appointed to be responsible for co-ordinating the information security arrangements of the network and act as a single point of contact on information security issues.

NW4.1.2

Local information security co-ordinator(s) should have:

a) a sound understanding of their information security roles and responsibilities
b) sufficient technical skills, time, tools (eg checklists and specialist software products) and authority to carry out their assigned role
c) access to in-house or external expertise in information security
d) documented standards / procedures to support day-to-day security activities
e) up-to-date information related to information security on issues (eg users' security requirements, emerging threats and newly discovered vulnerabilities) and techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture)
f) a channel of communication with the information security function.

NW4.1.3

The local information security co-ordinator(s) should meet regularly with the network owner to review the status of information security and agree security activities to be performed.

Section NW4.2 Security awareness

Principle Individuals maintaining the network should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure individuals maintaining the network apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.

NW4.2.1

There should be an information security policy that applies to the network. Network staff should be aware of, and comply with, the information security policy.

NW4.2.2

Network staff should:

a) take part in a security awareness programme (eg attend structured awareness training seminars)
b) be provided with information security education / training (eg using techniques such as presentations and computer-based training (CBT))
c) be supplied with specialised security awareness material, such as brochures, reference cards, posters and electronic documents delivered via the organisation's intranet.

Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities.

NW4.2.3

Network staff should be made aware of:

a) the meaning of information security (ie the protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the network
c) the importance of complying with information security policies and applying associated standards / procedures
d) their personal responsibilities for information security.

NW4.2.4

Network staff should be made aware that they are prohibited from:

a) unauthorised use of any part of the network
b) using the network (or network components) for purposes that are not work-related
c) making sexual, racist or other statements that may be offensive (eg when using e-mail, instant messaging, the Internet, or the telephone)
d) making obscene, discriminatory or harassing statements, which may be illegal (eg when using e-mail, instant messaging, the Internet, or the telephone)
e) downloading illegal material (eg with obscene or discriminatory content)
f) using unauthorised network components (eg using unauthorised third party software or modems)
g) unauthorised copying of information or software
h) disclosing confidential information (eg network designs or IP addresses) to unauthorised individuals
i) compromising passwords (eg by writing them down or disclosing them to others)
j) using personally identifiable information (ie information that can be used to identify an individual person) unless explicitly authorised
k) tampering with evidence in the case of information security incidents that may require forensic investigation.

(continued on the next page)

Section NW4.2 Security awareness (continued)

NW4.2.5

Network staff should be warned of the dangers of being overheard when discussing business information over the telephone or in public places (eg train carriages, airport lounges or bars).

Section NW4.3 Information classification

Principle Information transmitted over the network should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to the network, thereby preventing unauthorised disclosure.

NW4.3.1

Information transmitted over (or associated with) the network should be subject to an information classification scheme (ie a method of classifying information according to its level of confidentiality), which complies with enterprise-wide standards / procedures for information classification.

Some organisations also take into account requirements for integrity (ie the need for information to be valid, accurate and complete) and availability (ie the need for information to be accessible when required) when classifying information.

NW4.3.2

The information classification scheme should:

a) take account of the potential business impact from loss of confidentiality of information
b) be used to determine varying levels of confidentiality of information (eg top secret, company-in-confidence and public).

NW4.3.3

The information classification scheme should be used to classify:

a) information stored in paper form (eg contracts, plans and system documentation held in hard-copy form)
b) information transmitted across the network (eg business transactions, financial statistics, product design details and customer files)
c) electronic communication (eg e-mail and instant messaging).

Information classification typically involves labelling of:

- information stored in paper form (eg using rubber ink stamps, adhesive labels, hologram lamination)
- information stored in electronic form (eg using electronic watermarking, labelling headers and footers, using filename conventions)
- electronic communications (eg using digital signatures and including the classification in the subject header of e-mails).

NW4.3.4

Information classifications associated with the network should be:

a) signed off by an appropriate business representative
b) reviewed regularly and when changes are made to the network.

NW4.3.5

Information classification details associated with the network should be recorded in:

a) an inventory, or equivalent (eg a database, specialised piece of software, or on paper)
b) agreements with service providers (eg service level agreements).

(continued on the next page)

Section NW4.3 Information classification (continued)

NW4.3.6

Information classification details should include:

a) the classification of the information (eg top secret, company-in-confidence and public)
b) the identity of the information owner
c) a brief description of the information classified.

Section NW4.4 Information risk analysis

Principle The network should be subject to an information risk analysis on a regular basis, the results of which should be documented, reviewed and agreed.

Objective To identify key information risks associated with the network and determine the security controls required in order to keep those risks within acceptable limits.

NW4.4.1

The network should be subject to an information risk analysis, performed in accordance with enterprise-wide standards / procedures for information risk analysis, using a structured information risk analysis methodology.

Information risk analysis (sometimes referred to as simply risk analysis or risk assessment) is the identification, measurement and prioritisation of risk, and the selection of security controls to mitigate that risk. An example of a structured methodology is the ISF's Information Risk Analysis Methodology (IRAM).

NW4.4.2

The information risk analysis should take into consideration critical business applications supported by the network, and associated service level agreements (SLAs).

NW4.4.3

The information risk analysis should involve:

a) owners of critical business applications supported by the network
b) the network owner
c) a network specialist
d) key user representatives
e) an expert in risk analysis (eg a member of staff or a third party specialist who has appropriate experience as an information risk analysis practitioner)
f) an information security specialist (eg a member of staff or a third party specialist who has appropriate experience as an information security practitioner).

NW4.4.4

The information risk analysis should determine risk by assessing:

a) the potential level of business impact associated with the network
b) accidental and deliberate threats to the confidentiality, integrity or availability of information (eg denial of service attacks, malware, misusing systems to commit fraud, loss of power, malfunctions and human error) transmitted across the network
c) vulnerabilities due to control weaknesses
d) vulnerabilities due to circumstances that increase the likelihood of a serious information security incident occurring (eg use of the Internet, permitting third party access or siting a computer installation in an area prone to earthquakes or flooding).

NW4.4.5

The information risk analysis should take into account:

a) compliance requirements (eg legislation, regulation, industry standards and internal policies)
b) objectives of the organisation
c) information classification requirements
d) previous risk analyses conducted on the computer installation being assessed
e) characteristics of the operating environment of the application, network or computer installation being assessed.

(continued on the next page)

Section NW4.4 Information risk analysis (continued)

NW4.4.6

Results of the information risk analysis should be documented and include:

a) a clear identification of key risks
b) an assessment of the potential business impact of each risk
c) recommendations for the actions required to reduce risks to an acceptable level.

NW4.4.7

The information risk analysis should be used to help:

a) select the information security controls that will reduce the likelihood of serious information security incidents occurring
b) select information security controls that will satisfy relevant compliance requirements (eg the Sarbanes-Oxley Act 2002, the Payment Card Industry (PCI) Data Security Standard, Basel II 1998, data privacy requirements and anti-money laundering laws)
c) determine the costs of implementing security controls (eg costs associated with: design, purchase, implementation and monitoring of the controls; hardware and software; training; overheads, such as facilities; and consultancy fees)
d) evaluate the strengths and weaknesses of security controls
e) identify specialised security controls required by the network (eg encryption for sensitive information in transit).

NW4.4.8

Results of the information risk analysis (including risk treatment actions and any identified residual risk) should be:

a) communicated to the network owner and top management (eg board-level executives or equivalent)
b) signed off by an appropriate business representative.

Risk treatment typically involves one of four options: applying appropriate controls; accepting risks; avoiding risks; or transferring risks. Residual risk is that proportion of risk that still remains after selected controls have been implemented.

NW4.4.9

Information risk analyses of the network should be performed regularly and before major changes to the network are implemented.

Section NW4.5 Security audit / review

Principle The information security status of the network should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls have been implemented effectively, that information risk is being managed and to provide the network owner, and top management, with an independent assessment of the security status of the network.

NW4.5.1

Security audits / reviews of the network should be performed regularly and carried out independently of staff maintaining the network (eg by a third party specialist or internal audit).

NW4.5.2

Security audits / reviews of the network should:

a) assess the business risks associated with the network
b) consider the information security requirements of the business applications supported by the network.

NW4.5.3

Security audits / reviews of the network should assess the status of information security arrangements in key areas (eg network management, traffic management, network operations and local security management).

NW4.5.4

Security audits / reviews of the network should be:

a) agreed with the network owner
b) defined in scope, and documented
c) performed by experienced and qualified individuals who have sufficient technical skills and knowledge of information security
d) conducted frequently and thoroughly (in terms of scope and extent) to provide assurance that security controls function as required
e) focused on ensuring that controls are effective enough to reduce risks to acceptable levels
f) supplemented by the use of automated software tools
g) validated by competent individuals
h) complemented by reviews conducted by independent third parties.

NW4.5.5

Security audit / review activity should be managed by:

a) agreeing requirements for special processing routines or tests (eg network, system and application penetration testing) with the network owner
b) restricting access to the network by the audit / review team (eg by granting only 'read' access to business information and software files or other types of access only for isolated copies of business information and software files)
c) monitoring and logging the activities of the audit / review team
d) disposing of business information copied for the purpose of an audit / review as soon as it is no longer required (eg by erasure or physical destruction)
e) protecting software tools used in carrying out audits / reviews (eg by keeping them separate from tools / utilities used in the live environment and holding them in secure storage facilities, such as restricted software libraries)
f) protecting documents and system files relating to the audit / review.

(continued on the next page)

Section NW4.5 Security audit / review (continued)

NW4.5.6

Recommendations following security audits / reviews should be agreed with the network owner, and reported to top management (eg board-level executives or equivalent).

Area NW5
VOICE NETWORKS

Business processes can be disrupted if voice networks, such as telephone systems, are unavailable or overloaded. Harm can also be caused if voice networks are subject to unauthorised use by outsiders, or sensitive conversations are overheard. Accordingly, this area covers the security arrangements applied to traditional voice and Voice over IP (VoIP) networks.

Section NW5.1 Voice network documentation

Principle Voice networks should include documentation of essential components and be supported by documented standards / procedures.

Objective To provide employees with a clear statement of the security disciplines they are expected to follow in relation to voice networks.

NW5.1.1

There should be documented standards / procedures for voice networks, which cover:

a) use of the organisation's telephones
b) moves and changes of telephone users
c) registration and authentication of users with access to voice-mail
d) handling of threatening / abusive telephone calls
e) protection of the voice-mail system against unauthorised access (eg by use of password protection).

NW5.1.2

The configurations and settings for in-house telephone exchanges should be supported by accurate and complete documentation.

NW5.1.3

Telephones and associated wiring / cables should be documented in an up-to-date inventory.

Section NW5.2 Resilience of voice networks

Principle Voice networks should be supported by a robust and reliable set of hardware and software, and be supported by alternative facilities.

Objective To ensure that voice network facilities (eg telephone exchanges) are available when required.

NW5.2.1

In-house telephone exchanges should have:

a) sufficient capacity to cope with peak workloads
b) expansion / upgrade capabilities to cope with projected demand
c) alternative power supplies, such as batteries, to cope with brief power outages
d) a control and monitoring facility capable of providing reports on usage, traffic and response statistics.

NW5.2.2

In-house telephone exchanges should be protected by:

a) duplicate processors and function cards
b) emergency bypass, so that they can fall-back to direct calls
c) duplicate groups of exchange lines (to provide reliable links to network service providers)
d) access to alternative main exchanges operated by service providers
e) a source of power capable of coping with prolonged power failures.

NW5.2.3

Timely repair should be ensured by the use of maintenance contracts providing agreed response times for in-house telephone exchanges and operator consoles, and for telephone and associated wiring / cables.

NW5.2.4

Critical in-house telephone exchanges and associated operator consoles should be housed in environments that are physically secure.

NW5.2.5

Telephone wiring / cabling should be labelled, and protected from accidental damage or interception (eg by concealment and the use of armoured ducting).

NW5.2.6

Checks should be carried out to ensure the continuity of voice communications is addressed in:

a) IT contingency plans and arrangements associated with IT facilities accessible by the network
b) business continuity plans and arrangements associated with the business activities supported by the network.

Section NW5.3 Special voice network controls

Principle Voice network facilities (eg telephone exchanges) should be monitored regularly and access to them restricted.

Objective To prevent and detect unauthorised use or misuse of voice network facilities.

NW5.3.1

Access to operator consoles associated with in-house telephone exchanges should be restricted by the use of passwords (or equivalent), which are:

a) changed on installation, to ensure standard passwords set by the supplier cannot be exploited by unauthorised individuals
b) applied to the access ports used for remote diagnosis.

NW5.3.2

Changes to the configuration of settings for in-house telephone exchanges (including extension numbers) should be performed by authorised individuals.

NW5.3.3

Patterns of telephone use should be monitored to determine adequacy of the capacity of in-house telephone exchanges and operator workloads / staffing requirements.

NW5.3.4

Voice network bills / invoices should be inspected to identify unusual patterns of use which may indicate fraud or improper behaviour.

Section NW5.4 Voice over IP (VoIP) networks

Principle Voice over IP (VoIP) networks should be approved, and protected by a combination of general, network and VoIP-specific controls.

Objective To ensure the availability of the VoIP network, and protect the confidentiality and integrity of sensitive information (eg the content of telephone calls) in transit.

NW5.4.1

There should be documented standards / procedures for VoIP networks, which:

a) cover general network controls for VoIP (eg using bandwidth monitoring tools that are capable of recognising VoIP traffic, deploying network components to provide resilience and redundancy, implementing firewalls that can handle VoIP traffic or restricting devices that can access the VoIP network)
b) include VoIP-specific controls (eg separating voice traffic using virtual local area networks (LANs), hardening VoIP devices such as IP phones, routers and IP PBXs, scanning VoIP networks for vulnerabilities, encrypting sensitive VoIP traffic, and monitoring VoIP-related event logs)
c) prohibit the use of unauthorised VoIP technology (eg unauthorised connections to external VoIP services, such as Skype, using a software phone).

NW5.4.2

General network security controls for VoIP should include:

a) monitoring bandwidth using tools that are capable of recognising VoIP traffic
b) deploying network components to provide resilience and redundancy
c) implementing firewalls that can filter VoIP traffic
d) restricting access to the VoIP network to authorised devices.

NW5.4.3

VoIP-specific controls should include:

a) separating voice traffic using virtual local area networks (vLANs)
b) hardening VoIP devices (eg IP phones, routers and IP PBXs)
c) scanning VoIP networks for vulnerabilities
d) encrypting sensitive VoIP traffic
e) monitoring VoIP-related event log files.

Systems Development

Building security into systems during their development is more cost-effective and secure than applying it afterwards. It requires a coherent approach to systems development as a whole, and sound disciplines to be observed throughout the development cycle. Ensuring that information security is addressed at each stage of the cycle is of key importance.

Systems Development

SD1 Development Management

SD1.1 Roles and responsibilities

SD1.2 Development methodology

SD1.3 Quality assurance

SD1.4 Development environments

SD2 Local Security Management

SD2.1 Local security co-ordination

SD2.2 Security awareness

SD2.3 Security audit / review

SD3 Business Requirements

SD3.1 Specification of requirements

SD3.2 Confidentiality requirements

SD3.3 Integrity requirements

SD3.4 Availability requirements

SD3.5 Information risk analysis

SD4 Design and Build

SD4.1 System design

SD4.2 Application controls

SD4.3 General security controls

SD4.4 Acquisition

SD4.5 System build

SD4.6 Web-enabled development

SD5 Testing

SD5.1 Testing process

SD5.2 Acceptance testing

SD6 Implementation

SD6.1 System promotion criteria

SD6.2 Installation process

SD6.3 Post-implementation review

Area SD1
DEVELOPMENT MANAGEMENT

Producing robust systems, on which the organisation can depend, requires a sound approach to systems development. Accordingly, this area covers the organisation of systems development staff, the methodology used in developing systems, quality assurance and the security of development environments.

Section SD1.1 Roles and responsibilities

Principle An individual should be appointed to manage systems development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To achieve individual accountability for systems development activities and provide a sound management structure for staff performing them.

SD1.1.1

Overall responsibility for development activity should be clearly assigned to an individual (eg the head of systems development or a designated project manager). Business owners should be appointed to be responsible for particular development activities.

SD1.1.2

Responsibility for key tasks (eg compliance with development standards, quality assurance, definition of requirements, information risk analysis, design and build, testing and implementation) should be assigned to capable individuals, who should accept the responsibilities (including those for information security) associated with these roles.

SD1.1.3

The individuals involved in the development activities should have the skills, awareness and tools to:

a) develop systems effectively (eg to minimise security weaknesses)
b) design systems that can cope with error, exception and emergency conditions
c) integrate information security solutions.

SD1.1.4

The duties of development staff should be separated from the duties of staff running computers / networks in live environments.

SD1.1.5

Reliance on key individuals (for the security aspects of systems) should be minimised (eg by using standard development techniques / technologies, performing supervisory training and reviews, and arranging alternative cover, job rotation, and deputies).

Section SD1.2 Development methodology

Principle Development activities should be carried out in accordance with a documented system development methodology.

Objective To ensure that systems under development meet business requirements, including those for information security.

SD1.2.1

There should be a documented systems development methodology (often referred to as the system development life cycle (SDLC)).

SD1.2.2

The system development methodology should ensure that systems are developed to comply with:

a) enterprise-wide information security policy
b) enterprise-wide standards / procedures
c) legal and regulatory requirements
d) particular business requirements for security.

SD1.2.3

The system development methodology should include information security considerations during definition of requirements, design and build activity, the testing process and implementation activity.

SD1.2.4

The system development methodology should require the following activities to be performed at the start of each new project:

a) notification of the start of the project to the information security function (or equivalent)
b) creation of a risk register related to the project
c) creation of a project file.

SD1.2.5

Development staff should be trained in how to use the system development methodology.

SD1.2.6

The system development methodology should be:

a) kept up-to-date (eg to include new security methods and techniques)
b) applied by development staff in practice.

SD1.2.7

Compliance with the system development methodology should be monitored at key stages in the system development life cycle (eg during requirements, development, testing and deployment).

Section SD1.3 Quality assurance

Principle Quality assurance of key security activities should be performed during the system development life cycle.

Objective To provide assurance that security requirements are defined adequately, agreed security controls are developed, and security requirements are met.

SD1.3.1

Key security activities should be subject to quality assurance (eg spot checks to ensure compliance with system development methodologies and supervisory review of new staff or critical activities) during the systems development life cycle.

SD1.3.2

Quality assurance of key security activities should include:

a) assessing development risks (ie those related to running a development project, which would typically include risks associated with business requirements, benefits, technology, technical performance, costing and timescale)
b) checking that security requirements have been clearly defined
c) confirming that security controls (eg policies, methods, procedures, devices or programmed mechanisms intended to protect the confidentiality, integrity or availability of information) agreed during the information risk analysis process have been developed
d) determining if security requirements are being met effectively.

SD1.3.3

Quality assurance of key security activities should be:

a) performed at an early stage of the development process (typically before the design process)
b) reviewed at key stages during the development life cycle
c) documented.

SD1.3.4

The risk of developing insecure solutions should be minimised by:

a) revising project plans / resources if security requirements are not being met effectively (eg by changing or adding staff, amending plans, delaying timescales or revising costs)
b) cancelling systems development and installation activities if security requirements cannot be met satisfactorily (eg the discovery of significant vulnerabilities in the system).

Section SD1.4 Development environments

Principle System development activities should be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access.

Objective To provide a secure environment for system development activities, and avoid any disruption to mainstream business activity.

SD1.4.1

One or more systems development environments (eg a dedicated network or group of computer systems) should be established, in which development activities can be performed.

SD1.4.2

Development environments should be isolated from live environments (eg by hosting development systems on a standalone network or segregating the network using a firewall), and acceptance testing separated from development activity (eg by using a separate 'staging' environment).

SD1.4.3

Development environments should be protected by:

a) removing comments from programs (eg authentication details or sensitive information about the organisation) prior to deploying them in the live environment
b) preventing development staff from making unauthorised changes to live environments (eg by using access control software)
c) applying strict version control over systems development software (eg by using configuration management, recording access in a log and archiving old versions of software regularly)
d) employing malware detection / protection mechanisms
e) preventing malicious mobile code (eg executable code in the form of Java applets, MS ActiveX, JavaScript or VBScript, that has been written deliberately to perform unauthorised functions) from being downloaded into development environments (eg by the use of filtering or blocking techniques).

SD1.4.4

Assets within development environments (including software under development, business information used in the development process and important system documentation) should be protected against unauthorised access (eg by using logical and physical access control mechanisms).

SD1.4.5

Where access to third party source code (or equivalent) is not granted, a copy of the code should be:

a) maintained in escrow by a trusted third party (eg a lawyer, that holds the source code until fulfilment of the contract, or service level agreement (SLA) is fulfilled)
b) checked regularly to ensure it is up-to-date.

Area SD2
LOCAL SECURITY MANAGEMENT

In common with live systems, systems under development need to be supported by a sound organisational structure and run by individuals who are aware of information security and know how to apply security controls effectively. Accordingly, this area covers the arrangements made to ensure that information security is co-ordinated locally, systems development staff are aware of information security and understand their personal responsibilities, and the need for systems development activities to be subject to thorough, independent and regular security audits / reviews.

Section SD2.1 Local security co-ordination

Principle An individual should be appointed to co-ordinate information security activities associated with systems development.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that information security issues are resolved effectively.

SD2.1.1

An individual (eg the head of systems development), should have overall responsibility for information security associated with systems development activities. One or more local information security co-ordinators should be appointed to be responsible for co-ordinating the information security arrangements associated with systems development activities and to act as a single point of contact for information security issues.

SD2.1.2

Local information security co-ordinators should have:

a) a sound understanding of their information security roles and responsibilities
b) sufficient technical skills, time, tools (eg checklists and specialist software products) and authority to carry out their assigned roles
c) access to in-house or external expertise in information security
d) documented standards / procedures to support day-to-day security activities
e) up-to-date information on issues and techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture) related to information security
f) a channel of communication with the information security function (or equivalent).

SD2.1.3

The local information security co-ordinator(s) should meet regularly with the person in charge of the system(s) under development and relevant business owners to review the status of information security and agree information security activities to be performed.

Section SD2.2 Security awareness

Principle Systems developers should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure systems developers apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.

SD2.2.1

There should be an information security policy that applies to systems development activities. Systems development staff should be aware of, and comply with, the information security policy.

SD2.2.2

Systems development staff should:

a) take part in a security awareness programme (eg attend structured awareness training seminars)
b) be provided with information security education / training (eg using techniques such as presentations and computer-based training (CBT))
c) be supplied with specialised security awareness material (eg brochures, reference cards, posters and intranet-based electronic documents).

Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities.

SD2.2.3

System development staff should be made aware of:

a) the meaning of information security (ie protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect systems development activities
c) the importance of complying with information security policies and applying associated standards / procedures
d) their personal responsibilities for information security
e) particular security threats to the systems development activities (eg access violations, loss of power, system malfunctions, loss of services, overloads, and user errors).

SD2.2.4

Systems development staff should be made aware that they are prohibited from:

a) unauthorised use of information and systems (eg personal use of e-mail / Internet access and accessing particular business confidential information)
b) using systems for purposes that are not work-related (eg downloading games and audio / visual material from the Internet)
c) making sexual, racist or other statements that may be offensive (eg when using e-mail, instant messaging, the Internet, or the telephone)
d) making obscene, discriminatory or harassing statements, which may be illegal (eg when using e-mail, instant messaging, the Internet, or the telephone)
e) downloading illegal material (eg with obscene or discriminatory content)
f) unauthorised copying of information or software
g) compromising passwords (eg writing them down or disclosing them to others)
h) disclosing confidential information (eg development designs, IP addresses or details of external connections) to unauthorised individuals
i) using personally identifiable information (ie information that can be used to identify an individual person) unless explicitly authorised
j) tampering with evidence in the case of information security incidents that may require forensic investigation.

(continued on the next page)

Section SD2.2 Security awareness (continued)

SD2.2.5

Systems development staff should be warned of the dangers of being overheard when discussing business information associated with the development activity, over the telephone or in public places (eg train carriages, airport lounges or bars).

SD2.2.6

An information security awareness programme should be established specifically for systems development staff, to ensure that they are made aware of:

a) particular security threats to the systems development activities (eg access violations, loss of power, system malfunctions, loss of services, overloads, and user errors)
b) up-to-date secure coding practices
c) how to perform security tests.

SD2.2.7

Systems development staff should be provided with:

a) update and refresher training before and during systems development projects
b) access to information security resources (eg by making documentation available, and establishing a point of contact within the information security function for systems developers to use).

Section SD2.3 Security audit / review

Principle The information security status of systems development activity should be subject to thorough, independent and regular security audits / reviews.

Objective To ensure that security controls are designed effectively, that risk is managed, and to provide the business owner and top management, with an independent assessment of the information security status of systems development activities.

SD2.3.1

Security audits / reviews of systems development activities should be performed regularly and carried out independently of development staff (eg by a third party specialist or internal audit).

SD2.3.2

Security audits / reviews should:

a) assess the business risks associated with the systems development activities
b) consider the information security requirements of the system under development.

SD2.3.3

Security audits / reviews should assess the status of information security arrangements for:

a) development management (eg roles and responsibilities, development methodology and development environments)
b) local security management (eg local security co-ordination and security awareness)
c) business requirements (eg the specification of functional requirements, confidentiality requirements, integrity requirements, availability requirements and performing information risk analysis)
d) design and build (eg system design, acquisition, application controls, general security controls, system build and web-enabled development)
e) testing (eg the testing process and acceptance testing)
f) deployment (eg system promotion criteria, the installation process, post implementation review and decommissioning).

SD2.3.4

Security audits / reviews of systems development activities should be:

a) agreed with the person in charge of the system(s) under development
b) defined in scope, and documented
c) performed by experienced and qualified individuals (ie who have sufficient technical skills and knowledge of information security)
d) conducted frequently and thoroughly (in terms of scope and extent) to provide assurance that security controls function as required
e) focused on ensuring that controls are effective enough to reduce risks to acceptable levels
f) supplemented by the use of automated software tools
g) validated by competent individuals
h) complemented by reviews carried out by independent third parties.

(continued on the next page)

Section SD2.3 Security audit / review (continued)

SD2.3.5

Security audit / review activity should be managed by:

a) agreeing requirements for special processing routines (eg running a trace to track test transactions through systems) with the business owner
b) restricting access to the development environment by audit / review teams (eg by granting only 'read' access to business information and software files, or other types of access only for isolated copies of business information and software files)
c) monitoring and logging the activities of audit / review teams
d) disposing of business information copied for the purpose of audits / reviews, as soon as it is no longer required (eg by erasure or physical destruction)
e) protecting software tools used in carrying out audits / reviews (eg by keeping them separate from tools / utilities used in the live environment or holding them in secure storage facilities, such as restricted software libraries)
f) protecting documents and system files relating to audits / reviews.

SD2.3.6

Recommendations following security audits / reviews should be agreed with the person in charge of the system under development, and reported to top management (eg board-level executives or equivalent).

Area SD3
BUSINESS REQUIREMENTS

A thorough understanding of business requirements (including those for the confidentiality, integrity and availability of information) is essential if systems are to fulfil their intended purpose. Accordingly, this area covers the arrangements made for specifying business requirements, determining security requirements and conducting information risk analyses.

Section SD3.1 Specification of requirements

Principle Business requirements (including those for information security) should be documented and agreed before detailed design commences.

Objective To ensure that information security requirements are treated as an integral part of business requirements, fully considered and approved.

SD3.1.1

Business requirements for the system under development should be documented in a specification of business requirements (or equivalent) and supported by an agreed process for handling changes to requirements.

SD3.1.2

Business requirements should cover the need for system:

a) capacity (eg number of users or volume and size of transactions)
b) continuity (eg maximum length of time to recover key components following a system failure / outage)
c) flexibility (eg to support future developments or changes)
d) connectivity (eg interfaces to existing systems, networks or external resources)
e) compatibility (eg with particular technical environments or components).

SD3.1.3

Business requirements should cover the need for information:

a) processing (eg speed, and need for integrity)
b) storage (eg location, ease of access and need for confidentiality and availability)
c) transmission (eg source, destination, need for integrity and confidentiality).

SD3.1.4

Business requirements should cover:

a) compliance with contractual, legal and regulatory obligations
b) adherence to an information classification scheme (ie the method of classifying information according to its level of confidentiality)
c) the provision of arrangements to support the system in the live environment (eg the need for a helpdesk or technical support)
d) fall-back / contingency plans
e) the reduction or elimination of single-points-of-failure.

SD3.1.5

Business requirements should take into account existing information security policies, standards, procedures and guidelines.

(continued on the next page)

Section SD3.1 Specification of requirements (continued)

SD3.1.6

Business requirements should cover requirements for access by particular types of user (eg internal users, support staff, third parties or the general public), from particular locations (eg home offices or third party premises) and to particular types of information (eg creditcard details, personally identifiable information or trade secrets).

SD3.1.7

Business requirements should be signed off by the business owner of the system under development, an information security specialist, the person in charge of the system under development and the individual who will be responsible for maintaining the system in the live environment.

Section SD3.2 Confidentiality requirements

Principle The business impact of unauthorised disclosure of business information stored in or processed by the system under development should be assessed.

Objective To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the system under development.

SD 3.2.1

Business requirements should take account of the need to protect the confidentiality of information.

SD 3.2.2

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have a financial impact on the organisation in terms of:

a) loss of sales, orders or contracts (eg sales opportunities missed, orders not taken or contracts not signed)
b) loss of tangible assets (eg through fraud, theft of money or lost interest)
c) penalties / legal liabilities (eg through breach of legal, regulatory or contractual obligations)
d) unforeseen costs (eg recovery costs, uninsured losses, increased insurance)
e) depressed share price (eg sudden or prolonged loss of share value, or random share value fluctuation).

SD 3.2.3

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have an operational impact on the organisation in terms of:

a) loss of management control (eg impaired decision-making, inability to monitor financial positions, or process management failure)
b) loss of competitiveness (eg repetitive production line failures, degraded customer service or introduction of new pricing policies)
c) new ventures held up (eg delayed new products, delayed entry into new markets or delayed mergers / acquisitions)
d) breach of operating standards (eg contravention of regulatory, quality or safety standards).

SD 3.2.4

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have a customer-related impact on the organisation in terms of:

a) delayed deliveries to customers or clients (eg failure to meet product delivery deadlines or failure to complete contracts on time)
b) loss of customers or clients (eg customer / client defection to competitors or withdrawal of preferred supplier status by customer / client)
c) loss of confidence by key institutions (eg adverse criticism by investors, regulators, customers or suppliers)
d) damage to reputation (eg confidential financial information published in media, compromising internal memos broadcast by media).

SD 3.2.5

The analysis of confidentiality requirements should determine how the disclosure of confidential information could have an employee-related impact on the organisation in terms of:

a) reduction in staff morale / productivity (eg reduced efficiency, lost time or job losses)
b) injury or death (eg harm to staff).

Section SD3.3 Integrity requirements

Principle The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the system under development should be assessed.

Objective To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the system under development.

SD3.3.1

Business requirements should take account of the need to protect the integrity of information.

SD3.3.2

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have a financial impact on the organisation in terms of:

a) loss of sales, orders or contracts (eg sales opportunities missed, orders not taken or contracts not signed)
b) loss of tangible assets (eg through fraud, theft of money or lost interest)
c) penalties / legal liabilities (eg through breach of legal, regulatory or contractual obligations)
d) unforeseen costs (eg recovery costs, uninsured losses, increased insurance)
e) depressed share price (eg sudden or prolonged loss of share value, or random share value fluctuation).

SD3.3.3

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have an operational impact on the organisation in terms of:

a) loss of management control (eg impaired decision-making, inability to monitor financial positions, or process management failure)
b) loss of competitiveness (eg repetitive production line failures, degraded customer service or introduction of new pricing policies)
c) new ventures held up (eg delayed new products, delayed entry into new markets or delayed mergers / acquisitions)
d) breach of operating standards (eg contravention of regulatory, quality or safety standards).

SD3.3.4

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have a customer-related impact on the organisation in terms of:

a) delayed deliveries to customers or clients (eg failure to meet product delivery deadlines or failure to complete contracts on time)
b) loss of customers or clients (eg customer / client defection to competitors or withdrawal of preferred supplier status by customer / client)
c) loss of confidence by key institutions (eg adverse criticism by investors, regulators, customers or suppliers)
d) damage to reputation (eg confidential financial information published in media, compromising internal memos broadcast by media).

SD3.3.5

The analysis of integrity requirements should determine how the accidental corruption or deliberate manipulation of information could have an employee-related impact on the organisation in terms of:

a) reduction in staff morale / productivity (eg reduced efficiency, lost time or job losses)
b) injury or death (eg harm to staff).

Section SD3.4 Availability requirements

Principle The business impact of business information stored in or processed by the system under development being unavailable for any length of time should be assessed.

Objective To document and agree the availability requirements (the need for information to be accessible when required) of the system under development.

SD3.4.1

Business requirements should take account of the need to protect the availability of information.

SD3.4.2

The analysis of availability requirements should determine how the loss of availability of information could have a financial impact on the organisation in terms of:

a) loss of sales, orders or contracts (eg sales opportunities missed, orders not taken or contracts not signed)
b) loss of tangible assets (eg through fraud, theft of money or lost interest)
c) penalties / legal liabilities (eg through breach of legal, regulatory or contractual obligations)
d) unforeseen costs (eg recovery costs, uninsured losses, increased insurance)
e) depressed share price (eg sudden or prolonged loss of share value, or random share value fluctuation).

SD3.4.3

The analysis of availability requirements should determine how the loss of availability of information could have an operational impact on the organisation in terms of:

a) loss of management control (eg impaired decision-making, inability to monitor financial positions, or process management failure)
b) loss of competitiveness (eg repetitive production line failures, degraded customer service or introduction of new pricing policies)
c) new ventures held up (eg delayed new products, delayed entry into new markets or delayed mergers / acquisitions)
d) breach of operating standards (eg contravention of regulatory, quality or safety standards).

SD3.4.4

The analysis of availability requirements should determine how the loss of availability of information could have a customer-related impact on the organisation in terms of:

a) delayed deliveries to customers or clients (eg failure to meet product delivery deadlines or failure to complete contracts on time)
b) loss of customers or clients (eg customer / client defection to competitors or withdrawal of preferred supplier status by customer / client)
c) loss of confidence by key institutions (eg adverse criticism by investors, regulators, customers or suppliers)
d) damage to reputation (eg confidential financial information published in media, compromising internal memos broadcast by media).

(continued on the next page)

Section SD3.4 Availability requirements (continued)

SD3.4.5

The analysis of availability requirements should determine how loss of availability of information could have an employee-related impact on the organisation in terms of:

a) reduction in staff morale / productivity (eg reduced efficiency, lost time or job losses)
b) injury or death (eg harm to staff).

SD3.4.6

Business requirements should take into account the critical timescale of the application (ie the timescale beyond which an outage is unacceptable to the organisation).

Section SD3.5 Information risk analysis

Principle Systems under development should be subject to a structured information risk analysis, the results of which should be documented, reviewed and agreed.

Objective To identify key information risks associated with critical systems under development and determine the security controls required in order to keep those risks within acceptable limits.

SD3.5.1

Systems under development should be subject to an information risk analysis, which is performed in compliance with enterprise-wide standards / procedures for information risk analysis, using a structured information risk analysis methodology.

Information risk analysis (sometimes referred to as simply risk analysis or risk assessment) is the identification, measurement and prioritisation of risk, and the selection of security controls to mitigate that risk. An example of a structured methodology is the ISF's Information Risk Analysis Methodology (IRAM).

SD3.5.2

The information risk analysis should be:

a) performed at an early stage of the system development process (ie before the design process)
b) reviewed at key stages during the system development process.

SD3.5.3

The information risk analysis should involve:

a) the business owner (eg the individual in charge of the business function to be supported by the system under development)
b) the person in charge of the system under development
c) key user representatives
d) an IT specialist
e) an expert in information risk analysis (ie a member of staff or a third party specialist who has appropriate experience as an information risk analysis practitioner)
f) an information security specialist (eg a member of staff or a third party specialist who has appropriate experience as an information security practitioner).

SD3.5.4

The information risk analysis should determine risk by assessing:

a) the potential level of business impact associated with the system under development
b) accidental and deliberate threats to the confidentiality, integrity and availability of information (eg denial of service attacks, malware, misusing systems to commit fraud, loss of power, malfunctions and human error)
c) vulnerabilities due to control weaknesses
d) vulnerabilities due to circumstances that increase the likelihood of a serious information security incident occurring (eg use of the Internet, permitting third party access or siting a computer installation in an area prone to earthquakes and flooding).

(continued on the next page)

Section SD3.5 Information risk analysis (continued)

SD3.5.5

The information risk analysis should take into account:

a) compliance requirements (eg with legislation, regulation, contractual terms, industry standards and internal policies)
b) objectives of the organisation
c) information classification requirements
d) previous risk analysis conducted on the application being assessed
e) characteristics of the operating environment of the application, network or computer installation being assessed.

SD3.5.6

Results of the information risk analysis should be documented, and include:

a) a clear identification of key risks
b) an assessment of the potential business impact of each risk
c) recommendations for the actions required to reduce risk to an acceptable level.

SD3.5.7

The information risk analysis should be used to help:

a) select the security controls that will reduce the likelihood of serious information security incidents occurring, and satisfy relevant compliance requirements (eg Sarbanes-Oxley Act 2002, Basel II 1998, data privacy requirements, and anti-money laundering laws)
b) determine the costs of implementing security controls (eg costs associated with: design, purchase, implementation and monitoring of the controls; hardware and software; training; overheads, such as facilities; and consultancy fees)
c) evaluate the strengths and weaknesses of security controls
d) identify specialised security controls required by the system under development (eg encryption or strong authentication).

SD3.5.8

The results of the information risk analysis (including risk treatment actions and any identified residual risk) should be:

a) communicated to the person in charge of the system(s) under development and top management (eg board-level executives or equivalent)
b) signed off by the person in charge of development activity and the business owner of the system under development.

Risk treatment typically involves one of four options: applying appropriate controls; accepting risks; avoiding risks; or transferring risks. Residual risk is that proportion of risk that still remains after selected controls have been implemented.

SD

Area SD4
DESIGN AND BUILD

Building systems that function as intended requires the use of sound disciplines throughout the design and build stage of development. Accordingly, this area covers the arrangements needed to address information security during design, acquisition and system build, and the identification of required application, general and web-specific security controls.

Section SD4.1 System design

Principle Information security requirements for the system under development should be considered when designing the system.

Objective To produce a live system based on sound design principles which has security functionality built-in and enables controls to be incorporated easily.

SD4.1.1

The system design phase should involve:

a) analysis of the expected flow of information through the system under development (including: data inputs and connections to the system; transmission of data between system components; storage of information; access to databases and other types of storage; connections to other systems and applications; connections to application data from other systems; and security of information outputs)
b) consideration of the full range of security controls to protect live data (eg policies, methods, procedures, devices or programmed mechanisms intended to protect the confidentiality, integrity or availability of information)
c) identification of specific security controls required by particular business processes supported by the system under development (eg encryption of sensitive information)
d) evaluation of how and where security controls are to be applied (eg by developing a security architecture for the system under development)
e) review of designs to ensure security controls are specified, and are compliant with organisational security requirements
f) documentation of security controls that do not fully meet requirements
g) development of a security architecture that can support the technical system requirements, such as flexibility or scalability
h) consideration of how individual security controls (manual and automated) work together to produce an integrated set of controls.

SD4.1.2

Systems should be designed to:

a) provide 'defence in depth' (ie multiple layers of protection) to avoid reliance on one type or method of security control
b) assume input from external systems is insecure
c) repeat any client validation at the server, to defend against 'man in the middle' attacks
d) employ secure defaults
e) ensure key components 'fail securely' (ie in the event of a system failure, information is not accessible to unauthorised individuals, and cannot be tampered with or modified)
f) run with 'least privilege' (ie only the minimum possible privileges are granted to a user or a process when accessing the system, and not high-level privileges such as 'root' in UNIX systems or 'Administrator' in Windows systems).

(continued on the next page)

Section SD4.1 System design (continued)

SD4.1.3

The evaluation of alternative designs for the system under development should take into account the:

a) need to integrate with the existing security architecture
b) capability of the organisation to develop and support the chosen technology
c) cost of meeting security requirements
d) skills needed to develop required security controls (eg policies, methods, procedures, devices or programmed mechanisms intended to protect the confidentiality, integrity or availability of information).

SD4.1.4

Before coding or acquisition work begins, system designs should be documented, verified to ensure that they meet security requirements, reviewed by an information security specialist (eg to check that security architecture principles have been applied) and signed off by the person in charge of the system(s) under development.

Security architecture principles (sometimes referred to as guiding principles or design principles) represent fundamental security rules that should be met during the development of a security architecture for a system, and applied when the corresponding security controls are implemented.

Examples of security architecture principles include 'security by design', 'defence in depth', 'least privilege', 'default deny', and 'fail secure'.

SD

Section SD4.2 Application controls

Principle The full range of application controls should be considered when designing the system under development.

Objective To ensure that required application controls are built-in to the system under development.

SD4.2.1

The system design phase should include an assessment of possible application controls (eg devices or programmed mechanisms intended to protect the confidentiality, integrity or availability of information).

SD4.2.2

The assessment should include security controls associated with the validation of:

a) information entered (eg range checks, making key fields mandatory, control balances)
b) automated processes (eg record counts and / or hash, session, batch or balancing totals)
c) information integrity – the completeness, accuracy and validity of information (eg reconciliation with bank statements, customer / supplier records, or physical stock)
d) information output (eg reconciling control counts to ensure all data is processed or using plausibility checks to ensure output is reasonable)
e) changes to information (eg inspection of the contents of records before and after they have been changed).

SD4.2.3

The assessment should include security controls associated with the:

a) detection of unauthorised or incorrect changes to information (eg inspection of change logs, use of automated 'checksum' tools or reconciliation back to source)
b) protection of information from being accidentally overwritten (eg write-protecting key fields or files)
c) prevention of important internal information from being disclosed to unauthorised individuals (eg via application responses or error messages)
d) provision of error and exception reports
e) maintenance of event logs.

Section SD4.3 General security controls

Principle The full range of general security controls should be considered when designing the system under development.

Objective To ensure that required general security controls are established to support the system under development.

SD4.3.1

The system design phase should include an assessment of general security controls, including policies, methods, and standards / procedures, intended to protect the confidentiality, integrity and availability of information.

SD4.3.2

The assessment should cover security controls associated with user management, including:

a) definition of user roles, responsibilities and procedures
b) segregation of duties (eg dual control of payments)
c) access control functionality.

SD4.3.3

The assessment should cover cryptographic security controls associated with ensuring confidentiality, including encryption of:

a) key files / databases (eg using file-based, file system or hard disk encryption)
b) data in transit (eg via virtual private networks (VPNs) using protocols such as IPSec, SSL and TLS, and by encrypting electronic communications such as e-mail using PGP or X509 digital certificates).

SD4.3.4

The assessment should cover security controls associated with ensuring integrity, including:

a) minimisation of manual intervention (eg by automating processes)
b) prevention of unauthorised changes to software (eg malware protection, change management disciplines)
c) non-repudiation of the identity of an individual sending information (eg by using digital signatures).

SD4.3.5

The assessment should cover security controls associated with ensuring availability, including:

a) provision of adequate capacity to cope with normal / peak volumes of work
b) the reduction or elimination of single-points-of-failure
c) back-up arrangements (eg for business information and software)
d) fall-back / contingency plans.

Section SD4.4 Acquisition

Principle Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.

Objective To ensure that hardware and software acquired from third parties provides the required functionality and does not compromise the security of systems under development.

SD4.4.1

There should be documented standards / procedures for acquiring hardware / software, which apply to computer / network equipment, software packages, system software (eg operating systems, specialised tools and utilities) and specialised security products (eg malware protection software, intrusion detection and security event management).

SD4.4.2

Standards / procedures should specify:

a) guidelines for selecting hardware / software (eg lists of approved suppliers, security considerations and contractual terms)
b) methods of identifying and addressing security weaknesses in hardware / software
c) the need to meet software licensing requirements
d) the process for reviewing and approving hardware / software.

SD4.4.3

When acquiring hardware / software:

a) they should be selected from a list of approved suppliers
b) security requirements should be considered
c) a high priority should be placed on reliability in the selection process
d) contractual terms should be agreed with suppliers.

SD4.4.4

The risk of potential security weaknesses in hardware / software should be reduced by:

a) obtaining external assessments from trusted sources (eg auditor's opinions and specified security criteria, such as the 'Common Criteria' and Federal Information Processing Standards (FIPS))
b) identifying security deficiencies (eg by detailed inspection, reference to published sources, or by participating in user / discussion groups)
c) considering alternative methods of providing the required level of security (eg 'work-arounds').

SD4.4.5

Software licensing requirements should be met by obtaining adequate licenses for planned use and by providing proof of ownership of software (eg via 'blanket' licence agreements).

SD4.4.6

The acquisition of hardware / software should be reviewed by staff that have the necessary skills to evaluate them, and be approved by an appropriate business representative.

Section SD4.5 System build

Principle System build activities (including coding and package customisation) should be carried out in accordance with industry good practice; performed by individuals provided with adequate skills / tools; and inspected to identify unauthorised modifications or changes.

Objective To ensure that systems are built correctly, able to withstand malicious attacks, and that no security weaknesses are introduced during the build process.

SD4.5.1

There should be documented standards / procedures for building systems (eg program coding, web page creation, customisation of packages and defining data structures).

SD4.5.2

Standards / procedures for building systems should specify:

a) approved methods of building systems (eg defining competence levels for staff writing or reviewing code; customising software packages; and documenting changes)
b) mechanisms for ensuring systems comply with good practice for system design (eg the use of structured programming techniques, methods of secure coding and documenting code)
c) methods of managing the use of code samples (eg defining acceptable sources for developers to obtain sample code and requiring a security review of any sample code before it can be used in the system)
d) 'secure' methods of making changes to the base code of software packages
e) review and sign off processes (including those for software package customisation).

SD4.5.3

The build of system under development should be documented and inspected to identify unauthorised modifications or changes which may compromise security controls.

SD4.5.4

When building systems:

a) staff should comply with good practice for system coding (eg using structured programming techniques and documenting code)
b) the use of insecure design techniques should be prohibited (eg the use of hard coded passwords, unapproved code samples, web-enabled tools and database products)
c) development tools, such as Integrated Development Environments, should be configured to help enforce the creation of secure code
d) source code should be protected from unauthorised access and tampering (eg by using configuration management tools, which typically provide features such as access control and version control)
e) automated tools should be used to ensure adherence to coding standards.

SD4.5.5

Where modifications have to be made to the base code of third party software packages a documented process should be applied, which takes into account the risk of:

a) suppliers refusing to support or maintain modified software
b) built-in security controls being compromised
c) incompatibility with updated versions of the base software package.

(continued on the next page)

Section SD4.5 System build (continued)

SD4.5.6

The process should specify that modifications to the base code of third party software packages can only be made:

a) following approval by a systems development manager
b) with written permission from the supplier of the software package
c) to a clearly identified copy of the original code.

SD4.5.7

System build activities (eg application coding and package customisations) should be reviewed by a systems development manager to ensure that the system functions as intended and to confirm that security weaknesses have not been introduced (eg buffer overrun or SQL injection vulnerabilities).

SD4.5.8

Prior to release into the testing environment checks should be performed to ensure that:

a) application code functions correctly
b) vulnerabilities have been addressed
c) sensitive information (eg customer details) is removed from the application code.

SD4.5.9

System build activities should be signed off by the person in charge of the system under development.

Section SD4.6 Web-enabled development

Principle Specialised technical security controls should be applied to the development of web-enabled applications.

Objective To ensure that the increased risks associated with the development of web-enabled applications are minimised.

SD4.6.1

Additional controls should be employed when developing systems that will support web-enabled applications.

SD4.6.2

The business practices and privacy policies associated with website(s) that will support the application under development should be independently accredited (eg by organisations such as Web Trust or TRUSTe or equivalent).

SD4.6.3

The build process should ensure that the web server(s) that will support the application will be:

a) segregated from internal networks and untrusted networks (eg in a 'Demilitarised Zone' (DMZ))
b) run on one or more dedicated computers (ie they do not provide other services such as file and print, database or e-mail or other business applications)
c) run with 'least privilege' (eg excluding the use of high-level privileges, such as 'root' for UNIX systems or 'Administrator' for Windows systems)
d) prevented from initiating network connections to the Internet (eg through server configuration or by rules on a firewall)
e) configured so that scripts can only be run from specified locations
f) reviewed to ensure that all unnecessary software, network services and applications have been disabled / removed
g) configured to log security-related events generated by the website.

SD4.6.4

The build process should ensure that connections between web servers and back-office systems (eg application and database servers) will be:

a) protected by firewalls (eg stateful inspection firewalls (typically located in the perimeter of a network), application proxy firewalls (typically located between internal networks) and application firewalls (typically located close to the application))
b) limited to the services required by the application
c) restricted to code generated by web server applications (ie rather than by client applications)
d) based on documented application programming interfaces (APIs)
e) supported by mutual authentication (ie two computers verifying each other's identity before exchanging data).

SD4.6.5

User accounts on back-office systems that will be used by web servers to make connections should run with 'least privilege' (eg excluding the use of high-level privileges, such as 'root' for UNIX systems or 'Administrator' for Windows systems).

SD4.6.6

The build process should ensure that information used by the system under development will be subject to input validation at the server, in addition to that performed on the client application.

(continued on the next page)

Section SD4.6 Web-enabled development (continued)

SD4.6.7

The build process should ensure that website content will be:

a) stored on a separate partition / disk from the operating system
b) protected by setting file permissions, to prevent unauthorised access
c) updated only by authorised individuals and via approved methods (eg via CD at the web server console or transferring files using secure shell (SSH) or secure FTP from a predefined IP address)
d) reviewed to ensure that it is accurate, that hyperlinks are valid and functional, and that vulnerabilities have not been introduced by scripts or 'hidden' form fields.

SD4.6.8

Sensitive information in transit should be protected against disclosure by using encryption (eg using Secure Sockets Layer (SSL) or Transport Layer Security (TLS)) and by using HTTP PUT operations rather than GET operations.

SD4.6.9

Web application sessions should be protected against being hijacked or cloned by ensuring SessionIDs cannot be easily predicted (eg by using randomly generated SessionIDs), and by configuring the security parameters in 'cookies' used to hold session information.

SD4.6.10

The disclosure of information about the system configuration (that could be useful to hackers) should be prevented by:

a) suppressing or modifying the server field in HTTP headers that identify the web server's brand and version
b) ensuring that directories of files on web servers are not indexable
c) ensuring that the source code of server-side executables and scripts (eg Common Gateway Interface (CGI) scripts) cannot be viewed by a web browser
d) ensuring that the source of HTML, JavaScript and other client-side scripting languages do not contain unnecessary information (eg comments and details of web CGI functions).

SD4.6.11

Server-side executables and scripts (eg Common Gateway Interface (CGI) scripts and Internet Server Application Programming Interface (ISAPI) extensions and filters) should be configured to record actions performed.

Area SD5
TESTING

Testing is a fundamental element of good practice in systems development. Planned well and performed correctly, it provides assurance that systems, including security controls, function as intended and reduces the likelihood of system malfunctions occurring. Accordingly, this area covers the arrangements needed to carry out testing thoroughly, without disrupting other activities.

Section SD5.1 Testing process

Principle All elements of a system (including application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.

Objective To ensure systems function correctly and meet security requirements.

SD5.1.1

There should be a process for testing the system under development, which is supported by documented standards / procedures.

SD5.1.2

Standards / procedures for testing the system under development should cover:

a) the types of hardware, software and services to be tested
b) the use of test plans, including user involvement
c) key components of the testing process (eg the full functionality of business and security requirements; use under normal and exceptional business conditions; the impact of bad data; vulnerability to attack and the effectiveness of security controls)
d) documentation, review and sign off of the testing process.

SD5.1.3

Key components of new systems should be tested before being installed in the live environment, including application software packages, system software, hardware, communications services and environmental facilities (eg air conditioning and back-up power supplies).

SD5.1.4

New systems should be tested in accordance with predefined, documented test plans, which should be cross-referenced to the system design / specification to ensure complete coverage. Key user representatives should be involved in planning tests, and providing test data.

(continued on the next page)

Section SD5.1 Testing process (continued)

SD5.1.5

Tests should cover:

a) the full functionality of business requirements
b) use under normal and exceptional business conditions
c) use under exceptional conditions (eg conducting tests as at the year end)
d) error situations
e) vulnerability to attack (eg by simulating attacks and performing penetration tests to identify any vulnerabilities in the system under development)
f) the impact of bad data
g) interfaces with other systems (eg program calls or hyperlink references)
h) compatibility with applicable workstation configurations (eg running different operating systems, web browsers or third party software)
i) the effectiveness of security controls
j) identification of maximum system capacity (eg via stress testing)
k) system performance when handling planned volumes of working (ie load testing with realistic numbers of users / volumes of transactions)
l) fall-back arrangement (ie reversion to previous versions / procedures).

SD5.1.6

Automated tools should be used to improve the testing process (eg to check the validity of system interfaces or simulate loading from multiple clients).

SD5.1.7

There should be a process for ensuring that errors identified during the testing process are resolved in a consistent manner, which includes:

a) recording details of errors identified (eg in a test log or on a test results sheet)
b) assessing the associated risks
c) implementing mitigating actions
d) retesting the application.

SD5.1.8

Test results should be documented, checked against expected results, approved by users and signed off by an appropriate business representative.

Section SD5.2 Acceptance testing

Principle Systems under development should be subject to rigorous acceptance testing in a separate area that simulates the live environment.

Objective To ensure that newly developed systems function as intended and do not compromise information security.

SD5.2.1

Acceptance tests should be carried out for all new systems, in an environment that is separate from both the development and live environments and performed independently of system development staff.

SD5.2.2

Acceptance testing environments should be protected by:

a) restricting access to authorised users
b) applying change management practices.

SD5.2.3

Acceptance tests should:

a) involve business users
b) simulate the live environment
c) involve running the full suite of system components (including application functionality, database management utilities and the underlying operating system)
d) feature full integration testing, to ensure there will be no adverse effects on existing systems
e) involve independent security assessments of critical code, to detect vulnerabilities (eg 'back doors' or 'time bombs') and insecure use of programming features
f) include attempts to compromise the security of the system (eg by performing penetration tests).

SD5.2.4

Systems under development should be subject to:

a) penetration testing
b) access control testing
c) performance testing (ie under normal loads)
d) stress testing / volume testing (ie subjecting the system to large volumes of data to assess the performance under abnormal loads)
e) failure testing (eg to determine what happens if all or part of the system fails)
f) recovery testing
g) testing of manual fall-back or other contingency procedures.

SD5.2.5

Test data specifically designed to identify system faults or system weaknesses should be used during testing.

(continued on the next page)

Section SD5.2 Acceptance testing (continued)

SD5.2.6

Business information copied from the live environment for the purposes of conducting acceptance tests should be protected by:

a) prohibiting the use of personally identifiable information (ie information that can be used to identify an individual person) in the testing process
b) requiring separate authorisation each time business information is copied from the live into the testing environment
c) restricting access to business information in the testing environment
d) logging the use of business information
e) erasing copies of business information once testing is complete.

Area SD6
IMPLEMENTATION

Sound disciplines are required when new systems are promoted from the development into the live environment. Accordingly, this area covers system promotion criteria, the installation of new systems in the live environment and post-implementation reviews.

Section SD6.1 System promotion criteria

Principle Rigorous criteria should be met before new systems are promoted into the live environment.

Objective To ensure that only tested and approved versions of hardware and software are promoted into the live environment.

SD6.1.1

Documented acceptance criteria should be met before the new system is promoted into the live environment.

SD6.1.2

Before the new system is promoted into the live environment, checks should be performed to ensure that:

a) security assessments have been carried out
b) limitations of security controls have been documented
c) performance and capacity requirements can be met
d) all necessary patches and updates have been tested and successfully applied
e) all development problems have been resolved successfully
f) there will be no adverse effects on existing live systems
g) the security of the new system can be supported on a continuing basis (eg through a predefined point of contact such as a helpdesk)
h) arrangements for fall-back have been established, in the event of the new system(s) failing to function as intended
i) approval has been obtained from an appropriate business representative
j) test data (including business information) has been erased
k) service level agreements (SLAs) have been established to support the system.

A service level agreement (SLA) should include all key elements, such as: who is in charge of the application (ie the application owner); who is in charge of delivering the required service (eg an internal or external service provider); capacity requirements; maximum permissible down-time; criteria for measuring the level of service; and a warranty period for the system (to ensure support for the system after completion of its development).

SD6.1.3

Before the new system is promoted into the live environment:

a) error recovery and restart procedures should be established
b) contingency plans should be developed or updated
c) operating procedures should be tested
d) users should be educated to use the system correctly and securely
e) computer operators / system administrators should be trained in how to run the system correctly and securely.

(continued on the next page)

Section SD6.1 System promotion criteria (continued)

SD6.1.4

Security controls should be in place to ensure that only tested and approved versions of hardware and software are promoted into the live environment.

Section SD6.2 Installation process

Principle New systems should be installed in the live environment in accordance with a documented installation process.

Objective To minimise disruption to the organisation when new systems are installed in the live environment.

SD6.2.1

The promotion of new systems to the live environment should be governed by a documented installation process (or deployment plan).

SD6.2.2

The installation process should include:

a) validating the load or conversion of data
b) restricting the installation of new or significantly changed software to executable code
c) making users aware of their responsibilities for using the new system securely
d) providing ongoing technical support (eg via electronic help screens, a telephone helpdesk or hot-line support)
e) implementing new or revised standards / procedures
f) providing new or revised documentation
g) discontinuing old software, procedures and documentation
h) arranging for fall-back in the event of system failure
i) informing the individuals involved of their roles and responsibilities
j) handing over responsibility to individuals running the live environment
k) recording installation activity
l) archiving previous versions of software, together with corresponding information (including configuration settings, operations procedures, and supporting software).

SD6.2.3

The installation of new systems should be scheduled in advance, to avoid clashing with other activities (eg disrupting information processing activities).

Section SD6.3 Post-implementation review

Principle Post-implementation reviews should be conducted for all new systems.

Objective To check that systems and information security controls function as intended.

SD6.3.1

Post-implementation reviews should be conducted for all new systems.

SD6.3.2

Post-implementation reviews should cover:

a) fulfilment of business (including information security) requirements
b) the efficiency, effectiveness and cost of security controls
c) scope for improvement of security controls
d) information security incidents that occurred during system development.

SD6.3.3

The findings of post-implementation reviews should be signed off by the person in charge of the system under development, an appropriate business representative and an information security specialist.

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

End User Environment

Individuals in end user environments typically have access to corporate applications that are critical to the organisation and often develop critical desktop applications using powerful spreadsheets or databases. Furthermore, sensitive information can be processed or stored on local computing devices such as personal computers, hand-held devices or portable storage devices. Protecting this information is essential, and requires a combination of enterprise-driven and local activities, such as effective local security management; controlling access to corporate business applications; identifying and protecting important desktop applications; securing computing devices and electronic communications (eg e-mail, instant messaging and Internet access); and implementing effective business continuity arrangements.

End User Environment

UE1 Local Security Management

UE1.1 Roles and responsibilities

UE1.2 Security awareness

UE1.3 User training

UE1.4 Local security co-ordination

UE1.5 Information classification

UE2 Corporate Business Applications

UE2.1 Access control

UE2.2 Application sign-on process

UE2.3 Change management

UE3 Desktop Applications

UE3.1 Inventory of desktop applications

UE3.2 Protection of spreadsheets

UE3.3 Protection of databases

UE3.4 Desktop application development

UE4 Computing Devices

UE4.1 Workstation protection

UE4.2 Hand-held devices

UE4.3 Portable storage devices

UE5 Electronic Communications

UE5.1 General controls

UE5.2 E-mail

UE5.3 Instant messaging

UE5.4 Internet access

UE5.5 Voice over IP (VoIP) networks

UE5.6 Wireless access

UE6 Environment Management

UE6.1 Information privacy

UE6.2 Information security incident management

UE6.3 Back-up

UE6.4 Physical and environmental protection

UE6.5 Business continuity

Information Security Forum • Standard of Good Practice 2007

Area UE1
LOCAL SECURITY MANAGEMENT

Minimising information risks within the end user environment requires effective security management and the contribution of all individuals. Accordingly, this area covers roles and responsibilities, user awareness, and training. It also addresses local security co-ordination and information classification.

Section UE1.1 Roles and responsibilities

Principle An owner should be identified for the end user environment, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective To assign ownership of the end user environment, provide a sound management structure for staff and give responsible individuals a vested interest in the protection of the end user environment.

UE1.1.1

An individual should be appointed to take overall responsibility for managing the end user environment. Responsibilities of the individual should be assigned to a business manager, who should accept the responsibilities (including those for information security) associated with this role.

UE1.1.2

There should be documented standards / procedures covering systems used in the end user environment, approved by the individual in charge of the end user environment and kept up-to-date.

UE1.1.3

Standards / procedures should specify methods of:

a) administering users (eg adding new business users, updating access privileges, and revoking user access rights)
b) updating key 'static' business information (eg customer master files, currency exchange rates and product details)
c) monitoring key security-related events (eg system crashes, unsuccessful log-in of authorised users, and unsuccessful changes to access privileges)
d) processing information (eg data input, handling output and storing information)
e) using removable storage media (eg CDs, DVDs, external hard disk drives, flash memory cards and USB memory sticks)
f) validating processes / data
g) reviewing error / exception reports
h) identifying potential information security weaknesses / breaches.

UE1.1.4

Individuals involved in running or using systems within the end user environment should be:

a) assigned clear responsibilities
b) able to maintain systems correctly
c) capable of using applications and systems
d) competent to deal with error, exception and emergency conditions
e) aware of information security principles and associated good practice
f) sufficient in numbers to handle workloads at all times.

(continued on the next page)

Section UE1.1 Roles and responsibilities (continued)

UE1.1.5

Individuals involved in running and using systems in the end user environment should be organised to minimise:

a) reliance on key individuals (eg by arranging alternative cover or assigning deputies)
b) the risk of theft, fraud, error and unauthorised changes to information (eg by supervision of activities, prohibition of lone working and segregation of duties).

UE1.1.6

Terms and conditions of employment should:

a) state that information security responsibilities extend outside normal working hours and premises
b) state that information security responsibilities continue after employment has ended
c) explain the employee's legal responsibilities and rights (eg regarding copyright or data protection laws)
d) include a non-disclosure / confidentiality clause.

UE1.1.7

Staff should be required to accept terms and conditions of employment (eg contracts) in writing.

UE1.1.8

Staff employed in the end user environment should be screened prior to employment (eg by taking up references, checking career history, verifying academic qualifications and confirming identities).

UE1.1.9

External individuals working in the end user environment (eg consultants, contractors, engineers, and employees of third parties) should be:

a) required to sign a non-disclosure / confidentiality agreement
b) screened prior to employment (eg by taking up references, checking career history, checking academic qualifications and confirming identities).

UE1.1.10

There should be a documented requirement for access privileges to be revoked immediately when authorised users:

a) no longer require access as part of their job
b) leave the organisation.

Section UE1.2 Security awareness

Principle Users should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective To ensure users apply security controls and prevent important information from being compromised or disclosed to unauthorised individuals.

UE1.2.1

Internal staff and external individuals (eg consultants, contractors, engineers, and employees of third parties) working in the end user environment should be covered by an information security policy. They should be made aware of, and be able to demonstrate their compliance with the information security policy.

UE1.2.2

Users in the end user environment should:

a) take part in an information security awareness programme (eg attend structured awareness training seminars)
b) be provided with information security education / training (eg using techniques such as presentations and computer-based training (CBT))
c) be supplied with specialised information security awareness material (eg brochures, reference cards, posters and intranet-based electronic documents).

Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organisation and their individual security responsibilities.

UE1.2.3

Users in the end user environment should be made aware of:

a) the meaning of information security (ie protection of the confidentiality, integrity and availability of information)
b) why information security is needed to protect the end user environment, and the organisation
c) the importance of complying with the information security policy, and applying associated standards / procedures
d) their personal responsibilities for information security.

UE1.2.4

Users should be warned of the dangers of being overheard when discussing business information over the telephone and in public places (eg train carriages, airport lounges or bars).

UE1.2.5

Users in the end user environment should be made aware of the information risks specific to:

a) corporate business applications (eg sales order processing software, customer relationship management software, stock control programs and financial and accounting packages)
b) desktop applications (eg those developed using spreadsheet and database programs and used to support critical business processes such as high value transactions, processing important information and managing a production line)
c) working with electronic information (eg e-mails and electronic files such as letters, reports and contracts)
d) handling information in paper form.

(continued on the next page)

Section UE1.2 Security awareness (continued)

UE1.2.6

Users in the end user environment should be made aware that they are prohibited from:

a) unauthorised use of information and systems
b) using information and systems for purposes that are not work-related (eg downloading games and audio / visual material from the Internet)
c) making sexual, racist or other statements that may be offensive (eg when using e-mail, instant messaging, the Internet, or the telephone)
d) making obscene, discriminatory or harassing statements, which may be illegal (eg when using e-mail, instant messaging, the Internet, or the telephone)
e) downloading illegal material (eg with obscene or discriminatory content)
f) using unauthorised system or application components (eg installing unauthorised third party software, modems or wireless network interface cards (NICs))
g) unauthorised copying of information or software
h) compromising passwords (eg by writing them down or disclosing them to others)
i) disclosing confidential information to unauthorised individuals (eg customer records, product designs and pricing policies)
j) using personally identifiable information (ie information that can be used to identify an individual person) unless explicitly authorised
k) tampering with evidence in the case of information security incidents that may require forensic investigation.

UE1.2.7

Users in the end user environment should be made aware of the:

a) requirement to implement security controls over desktop applications (eg access control mechanisms, malware protection software and back-up programs)
b) need for segregation of duties / roles and processes (eg by defining and implementing roles, authorities, responsibilities and processes for issues such as ownership, 'sign off' and usage).

Section UE1.3 User training

Principle Users should be trained in how to run systems correctly and how to develop and apply security controls.

Objective To provide users with the skills required to protect systems and fulfil their information security responsibilities.

UE1.3.1

Users in the end user environment should be provided with training related to information systems, which includes how to use:

a) corporate business applications (eg sales order processing software, customer relationship management software, stock control programs, and financial and accounting packages)
b) desktop applications (eg those developed using spreadsheet and database programs and used to support critical business processes such as high value transactions, processing important information and managing a production line).

UE1.3.2

Users should be made aware of the security features provided with corporate business applications and desktop applications (eg encryption, access controls and password protection).

UE1.3.3

Users should be trained in how to create and protect electronic files (eg by defining access rights, and using encryption and password protection).

Section UE1.4 Local security co-ordination

Principle An individual should be appointed to co-ordinate information security activities in the end user environment.

Objective To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

UE1.4.1

Responsibility for information security should be assigned to the individual in charge of the end user environment. A local information security co-ordinator should be appointed with responsibility for co-ordinating information security arrangements within the end user environment.

UE1.4.2

The local information security co-ordinator should act as a single point of contact on information security issues and be supported by the individual in charge of the end user environment.

UE1.4.3

Local information security co-ordinator(s) should have:

a) a sound understanding of their information security roles and responsibilities
b) sufficient technical skills to carry out their assigned roles
c) the time to carry out their assigned roles
d) necessary tools (eg checklists and specialist software products)
e) sufficient authority to carry out their assigned roles
f) access to in-house or external expertise in information security
g) documented standards / procedures to support day-to-day security activities
h) up-to-date information related to information security issues (eg users' security requirements, emerging threats and newly discovered vulnerabilities) and techniques (eg information risk analysis methodologies, forensic investigation software and an enterprise-wide security architecture)
i) a channel of communication with the information security function.

UE1.4.4

Local information security co-ordinator(s) should meet regularly with the individual in charge of the end user environment to:

a) review the status of information security associated with the end user environment
b) agree information security activities to be performed.

Section UE1.5 Information classification

Principle Information stored in or processed by applications and systems in the end user environment should be classified according to its confidentiality, using an approved information classification scheme.

Objective To determine the level of protection that should be applied to applications and systems in the end user environment, thereby preventing unauthorised disclosure.

UE1.5.1

There should be an information classification scheme (ie the method of classifying information according to its level of confidentiality) that applies to information associated with the end user environment.

Some organisations also take into account the requirements for information integrity (ie the need for information to be valid, accurate and complete) and information availability (ie the need for information to be accessible when required) when classifying information.

UE1.5.2

The information classification scheme should:

a) comply with enterprise-wide standards / procedures for information classification
b) take account of the potential business impact from the loss of confidentiality of information
c) determine varying levels of confidentiality of information (eg top secret, company-in-confidence and public).

UE1.5.3

The information classification scheme should be used to classify:

a) information stored in paper form (eg contracts, plans and system documentation held in hard-copy form)
b) information stored in electronic form (eg business transactions, financial statistics, product design details and customer files)
c) electronic communications (eg messages sent via e-mail and instant messaging).

Information classification typically involves labelling of:

- information stored in paper form (eg using rubber ink stamps, adhesive labels, hologram lamination)
- information stored in electronic form (eg using electronic watermarking, labelling headers and footers, using filename conventions)
- electronic communications (eg using digital signatures and including the classification in the subject header of e-mails).

UE1.5.4

Classifications of information associated with the end user environment should be performed regularly and signed off by an appropriate business representative (eg the individual in charge of a business process or activity).

UE1.5.5

Information classification details should be recorded in an inventory (or equivalent), which includes:

a) the classification of the information (eg top secret, company-in-confidence and public)
b) the identity of the information owner
c) a brief description of the information classified.

Area UE2
CORPORATE BUSINESS APPLICATIONS

Corporate business applications accessible from the end user environment should be protected from unauthorised access and the adverse consequences of change. Accordingly, this area covers the disciplines required to restrict access to corporate business applications and to ensure that changes made do not cause adverse business impact.

Section UE2.1 Access control

Principle Access to corporate systems should be restricted to authorised individuals.

Objective To ensure that only authorised individuals are granted access to corporate systems, and that individual accountability is assured.

UE2.1.1

Users of corporate business applications should:

a) be uniquely identified (eg by a UserID), and authenticated (eg by a password or token)
b) maintain the confidentiality of authentication information (eg passwords and PINs).

UE2.1.2

There should be a process for issuing and managing system passwords used by individuals within the end user environment, which:

a) ensures that disclosure of the password is minimised when it is communicated to the user (eg by using encrypted e-mails or forcing the user to change the password when it is used for the first time)
b) involves the target user directly (ie the person to whom the password uniquely applies)
c) verifies the identity of the target user
d) ensures passwords are changed regularly.

UE2.1.3

Access to critical business applications should involve the use of strong authentication mechanisms (eg smartcards, tokens and biometrics such as fingerprint recognition).

UE2.1.4

Access controls should be applied (either manually or through automated means) to users to ensure individual accountability (eg 'read-only' for some files and no execute for some features).

UE2.1.5

Users' access rights should be restricted according to approved standards / procedures, and access restricted according to a defined policy (eg a 'need-to-know' or 'need-to-restrict' basis).

(continued on the next page)

Section UE2.1 Access control (continued)

UE2.1.6

User access privileges should be:

a) restricted according to the users' individual roles
b) signed off by the individual with overall responsibility for managing the end user environment
c) revoked promptly when an individual user is no longer entitled to them (eg when changing job or leaving the organisation).

Section UE2.2 Application sign-on process

Principle Users should be subject to a rigorous sign-on process before they are provided with access to corporate business applications.

Objective To ensure that only authorised users are granted access to corporate business applications.

UE2.2.1

There should be a sign-on process that users must follow before they can gain access to corporate business applications. The process should enable individual users to be uniquely identified (eg by using unique UserIDs).

UE2.2.2

Sign-on mechanisms should be configured so that they:

a) limit the number of unsuccessful sign-on attempts which are permitted (eg after three unsuccessful login attempts the user is disconnected)
b) restrict additional sign-on attempts (eg by forcing a time delay before sign-on can be re-tried or by revoking the UserID)
c) limit the duration of any one sign-on session
d) are re-enabled automatically after interruption (eg following a disconnection from the application).

UE2.2.3

Sign-on mechanisms should be configured to provide information so that they:

a) display no identifying details until sign-on is completed successfully
b) warn that only authorised users are permitted access.

UE2.2.4

The approval of the individual in charge of the end user environment should be obtained before any important features of sign-on processes are bypassed, disabled or changed.

Section UE2.3 Change management

Principle Changes to corporate business applications accessible from the end user environment should be tested, reviewed and applied using a change management process.

Objective To ensure that changes are applied correctly and do not compromise security.

UE2.3.1

There should be a change management process that applies to corporate business applications used within the end user environment.

UE2.3.2

The change management process should cover all types of change (eg upgrades and modifications to applications and software, revisions to parameter tables and settings, modifications to business information, changes to user / operating procedures, emergency 'fixes', and changes to the computers / networks that support the end user environment).

UE2.3.3

The change management process should be documented, and include:

a) approving and testing changes to ensure that they do not compromise security controls
b) performing changes and signing them off to ensure they are made correctly and securely
c) reviewing completed changes to ensure that no unauthorised changes have been made.

UE2.3.4

Prior to changes being applied change requests should be:

a) accepted only from authorised individuals
b) documented (eg on a change request form)
c) approved by an appropriate business representative
d) assessed for the potential business impact of changes.

UE2.3.5

Changes to corporate business applications within the end user environment should be:

a) performed by skilled and competent individuals who are capable of making changes correctly and securely
b) supervised by an IT specialist
c) signed off by an appropriate business representative.

UE2.3.6

Arrangements should be made to ensure that once changes have been applied:

a) version control is maintained (eg using configuration management)
b) a record is maintained, showing what was changed, when, and by whom (eg using automated helpdesk / service desk software)
c) details of changes are communicated to relevant individuals (eg associated users, business managers and relevant third parties)
d) checks are performed to confirm that only intended changes have been made (eg by using code comparison programs or checking 'before and after' contents of key records, such as within customer master files)
e) documents associated with the corporate business application are updated (eg design information, system configuration, implementation details, and records of all changes to the application)
f) the classification of information associated with the corporate business application is reviewed.

(continued on the next page)

Section UE2.3 Change management (continued)

UE2.3.7

There should be a documented method for applying emergency fixes to desktop applications (eg when the change management process cannot be followed and business impact needs to be minimised).

UE2.3.8

Emergency fixes should be:

a) approved by the individual responsible for managing the end user environment
b) logged (eg to support the follow-up activities performed after the emergency is over).

UE2.3.9

Once the emergency is over, emergency fixes should be:

a) reviewed by an appropriate business representative
b) documented
c) subject to standard change management disciplines (eg retrospective testing to ensure the emergency fix does not have a future impact on the organisation)
d) checked to ensure that they are not permanently left in place.

Area UE3
DESKTOP APPLICATIONS

Protecting critical desktop applications in the end user environment, and the accuracy of the information they store or process, requires a combination of good practice in general information security, supported by a set of technical security controls specific to desktop applications. Accordingly, this area covers the recording of critical desktop applications in an inventory, the development of critical desktop applications, and their protection.

Section UE3.1 Inventory of desktop applications

Principle Critical desktop applications used in the end user environment should be recorded in an inventory, or equivalent.

Objective To maintain an accurate and up-to-date record of critical desktop applications in the end user environment, enabling them to be protected accordingly.

UE3.1.1

Details of critical desktop applications (eg those developed using spreadsheet and database programs and used to support critical business processes such as high value transactions, processing important information and managing a production line) should be recorded in an inventory, or equivalent.

Desktop applications are typically developed using spreadsheet programs, (eg Microsoft Excel, OpenOffice Calc or Lotus 1-2-3) or database programs, (eg Microsoft Access, OpenOffice Base or Lotus Approach) or similar.

UE3.1.2

Details recorded in the inventory should include:

a) a description of each critical desktop application
b) the identity of the individual with primary responsibility for maintaining and using each critical desktop application
c) details of the intended purpose of each critical desktop application (eg processing of: operational information, such as tracking and monitoring operational workflow; analytical / management information to support decision-making; or financial information such as balances populated in a general ledger)
d) the type of information processed by each critical desktop application (eg customer details, product data or financial transaction information)
e) the department / individual responsible for the development of each critical desktop application (eg individuals in the end user environment or an IT function that specialises in spreadsheet and database programs)
f) any changes made to each critical desktop application.

UE3.1.3

The inventory should include details about the level of complexity of each critical desktop application, such as:

a) low (eg desktop applications that are used to maintain basic lists)
b) moderate (eg desktop applications that perform simple calculations or provide information for analytical review)
c) high (eg desktop applications that support complex calculations, valuations and modelling tools).

(continued on the next page)

Section UE3.1 Inventory of desktop applications (continued)

UE3.1.4

The inventory of critical desktop applications should be:

a) kept up-to-date
b) checked for accuracy on a regular basis (eg to ensure that content is complete, comprehensive, correct and timely)
c) signed off by an appropriate business representative.

Section UE3.2 Protection of spreadsheets

Principle Critical desktop applications created using spreadsheet programs should be protected by validating input, implementing access control, and restricting access to powerful functionality.

Objective To assure the accuracy of information processed by critical spreadsheets, and protect that information from disclosure to unauthorised individuals.

UE3.2.1

Critical spreadsheets should be supported by documented standards / procedures, which cover:

a) training of individuals that use spreadsheets
b) validation of information input into spreadsheets
c) protection of spreadsheets and the information they contain.

Critical spreadsheets are often developed using spreadsheet programs (eg Microsoft Excel, OpenOffice Calc or Lotus 1-2-3). Often, macros (which are small, user defined, routines or pieces of code) are developed within the spreadsheet to automate functions like routine tasks, importing data, performing calculations and creating new menus and shortcuts.

UE3.2.2

Individuals that use and develop critical spreadsheets should be trained in how to:

a) use them effectively
b) protect the information they store and process
c) develop additional functionality in spreadsheets (eg writing macros, conducting error checking and performing calculations in cells).

UE3.2.3

Information input into critical spreadsheets should be validated using validation routines, which:

a) require particular spreadsheet cells to contain a non-null value (ie the cell contains a value of some type, and is not empty)
b) restrict the type of information entered (eg requiring entered information to be in the format of date, currency, number or text)
c) use range checks to ensure information entered into the spreadsheet is within a predefined range (eg checking that a number that should be positive, is not negative)
d) generate hash totals, to allow the integrity of information to be checked at various stages of being processed
e) perform consistency checks (eg on a formula that is repeated throughout a spreadsheet).

UE3.2.4

The risk of inaccurate entry of information should be reduced by the use of:

a) default values (eg pre-agreed values that will automatically be entered when a new record is added)
b) drop-down lists consisting of predefined values (eg to help users of spreadsheets select the correct information)
c) error messages (eg error codes and descriptive text provided to inform users when a mistake may have occurred)
d) special coding routines to check input values (eg macros and automated error checking routines).

(continued on the next page)

Section UE3.2 Protection of spreadsheets (continued)

UE3.2.5

Critical spreadsheets should be protected by:

a) storing them on a central server (eg to reduce the risk of accidental and deliberate modification, and to help ensure spreadsheets are backed-up centrally)
b) limiting access to authorised individuals (eg by using password protection and creating access control lists that limit access to spreadsheets or folders that contain spreadsheets)
c) assigning privileges to restrict the functions authorised individuals can perform in spreadsheets (eg by defining different passwords for separate functions, such as opening, reading and modifying spreadsheets)
d) using only approved versions of spreadsheets (eg using the current spreadsheet version, or an approved spreadsheet program such as Microsoft Excel, OpenOffice Calc or Lotus 1-2-3).

UE3.2.6

The integrity of information contained in spreadsheets should be assured by:

a) using separate areas for calculation cells and data entry cells
b) restricting access to calculation areas (eg by using passwords)
c) conducting reconciliations of information entered into the spreadsheet (eg by manually checking against source information or physical records, or by implementing an automated process that checks information as it is downloaded or transferred from another application)
d) restricting access to, or removing standard menus (eg by hiding the standard menus or replacing standard menus with a customised menu to prevent access to developer functions)
e) restricting changes to coding routines that are used to produce additional functionality developed in the spreadsheet (eg writing macros, conducting error checking or performing calculations in cells).

Section UE3.3 Protection of databases

Principle Critical desktop applications created using database programs should be protected by validating input, implementing access control, and restricting access to powerful functionality.

Objective To assure the accuracy of information processed by critical databases, and protect that information from disclosure to unauthorised individuals.

UE3.3.1

Critical databases should be supported by documented standards / procedures, which cover:

a) training of individuals that use databases
b) validation of information input into databases
c) protection of databases and the information they contain.

Critical databases are often developed using commercial-off-the-shelf (COTS) database programs (eg Microsoft Access, OpenOffice Base or Lotus Approach).

UE3.3.2

Individuals that use and develop critical databases should be trained in how to:

a) use them effectively
b) protect the information they store and process
c) develop functionality in databases.

UE3.3.3

Information input into critical databases should be validated using validation routines, which:

a) require particular database fields to contain a non-null value (ie the field contains a value of some type, and is not empty)
b) restrict the type of information entered (eg requiring entered information to be in the format of date, currency, number or text)
c) use range checks to ensure information entered into the database is within a predefined range (eg checking that a number that should be positive, is not negative)
d) generate hash totals, to allow the integrity of information to be checked at various stages of being processed
e) perform consistency checks (eg on a calculation that is repeated throughout a database).

UE3.3.4

The risk of inaccurate entry of information should be reduced by the use of:

a) default values (eg pre-agreed values that will automatically be entered when a new record is added)
b) drop-down lists consisting of predefined values (eg to help users of databases select the correct information)
c) error messages (eg error codes and descriptive text provided to inform users when a mistake may have occurred).

UE3.3.5

The integrity of information in the database should be protected by employing data concurrency methods, to ensure that information is not corrupted when modified by more than one user.

(continued on the next page)

Section UE3.3 Protection of databases (continued)

UE3.3.6

Critical databases should be protected by:

a) storing them on a central server (eg to reduce the risk of accidental and deliberate modification, and to help ensure databases are backed-up centrally)
b) limiting access to authorised individuals (eg using password protection and creating access control lists to limit access to databases or folders that contain databases)
c) assigning privileges to restrict the functions authorised individuals can perform in databases (eg defining user profiles and user privileges for individuals that need to open, read and modify the contents of databases)
d) using only approved versions of databases (eg using the current database version, or an approved database program, such as Microsoft Access, OpenOffice Base or Lotus Approach)
e) using passwords to limit access to critical databases.

UE3.3.7

Source code (or equivalent) should be protected by compiling databases.

UE3.3.8

Access to database functionality should be restricted (eg using password protection to prevent unauthorised creation of declarations, statements, and procedures that perform operations or calculate values within a database).

UE3.3.9

Information contained in databases should be protected by restricting access to, or removing standard menus (eg by hiding the standard menus or replacing standard menus with a customised menu to prevent access to developer functions).

Section UE3.4 Desktop application development

Principle Development of desktop applications should be carried out in accordance with a documented development methodology.

Objective To ensure desktop applications function correctly and meet security requirements.

UE3.4.1

There should be documented standards / procedures for developing critical desktop applications, which cover: specifying requirements; designing, building and testing the desktop application; distributing the desktop application; and training users of the desktop application.

UE3.4.2

Development of critical desktop applications should include a definition of security requirements, which:

a) includes an assessment of the need for confidentiality, integrity and availability of information
b) takes into account an information classification scheme (ie the method of classifying information according to its level of confidentiality such as top secret, company-in-confidence and public).

UE3.4.3

Security requirements for critical desktop applications should be documented and signed off by an appropriate business representative (eg the individual in charge of the end user environment).

UE3.4.4

Critical desktop applications should be subject to information risk analysis, in accordance with enterprise-wide standards / procedures for information risk analysis (eg using a structured Information Risk Analysis Methodology, such as the ISF's IRAM approach).

UE3.4.5

The results of the information risk analysis should be signed off by an appropriate business representative.

UE3.4.6

The design of critical desktop applications should include the identification and selection of security controls.

UE3.4.7

The build of critical desktop applications should be subject to:

a) approved methods of developing desktop applications (eg when creating macros and similar user defined routines in spreadsheets, databases, and other desktop applications)
b) documented version control (eg by using incremental version numbers following a change to the desktop application)
c) review by an independent desktop application specialist (eg an individual that does not work in the end user environment, and is highly skilled in the functionality of desktop applications).

UE3.4.8

Critical desktop applications should be tested to ensure that they:

a) function as required
b) meet security requirements.

(continued on the next page)

Section UE3.4 Desktop application development (continued)

UE3.4.9

Testing of critical desktop applications should be supplemented by the use of automated tools (eg macros, defined routines and scanning tools) to examine the integrity of formulae and code.

UE3.4.10

Before critical desktop applications are made available to users, checks should be performed to ensure that they can be supported on a continuing basis (eg by an individual or group of individuals skilled in developing desktop applications).

UE3.4.11

Changes to critical desktop applications should be:

a) performed in accordance with a change management process
b) reviewed to ensure that they do not adversely affect intended functionality or compromise security controls.

Area UE4
COMPUTING DEVICES

The protection of computing devices used in the end user environment (and the information they store or process) requires a combination of both physical and logical controls to be applied. Accordingly, this area covers the disciplines required to configure, maintain and protect workstations, hand-held devices and portable storage devices.

Section UE4.1 Workstation protection

Principle Workstations used in the end user environment should be purchased from approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical and logical controls.

Objective To ensure workstations operate as intended, are available when required and do not compromise the security of information stored in or processed by them.

UE4.1.1

Workstations (ie desktop computers and laptop computers) used in the end user environment should be:

a) supported by maintenance arrangements
b) protected by physical and environmental controls (eg locks, alarms and indelible markings)
c) provided with standard, technical configurations (eg pre-configured with a standard operating system, standard applications and common communications software).

UE4.1.2

Workstations should be protected by the use of:

a) a comprehensive set of system management tools (eg maintenance utilities, monitoring software, discovery tools and back-up software)
b) access control mechanisms (ie to restrict access to the workstation)
c) up-to-date malware protection software, to protect against malicious software (eg computer viruses, worms, trojan horses, spyware, adware and malicious mobile code)
d) automatic time-out after a set period of inactivity
e) encryption software to safeguard information stored on internal and external hard disk drives.

UE4.1.3

Portable devices such as laptop computers should be protected against theft by:

a) providing users with physical locks or equivalent security devices
b) the use of indelible marking
c) attaching identification labels.

Section UE4.2 Hand-held devices

Principle Hand-held devices (eg Personal Digital Assistants (PDAs), WAP-based mobile phones and smartphones) used in the end user environment should be approved, protected by software controls and supported by standards / procedures for acceptable use.

Objective To ensure hand-held devices operate as intended, are available when required and do not compromise the security of information stored in or processed by them.

UE4.2.1

The use of hand-held devices should be authorised, and supported by maintenance arrangements.

UE4.2.2

Hand-held devices should be protected by the use of:

a) standard, technical configurations (eg pre-configured to run a standard operating system, standard applications and common communications software)
b) access control mechanisms (eg to restrict access to hand-held devices by using PIN codes or passwords)
c) up-to-date malware protection software, to protect against malicious software (eg computer viruses, worms, trojan horses, spyware, adware and malicious mobile code)
d) encryption software to safeguard information stored on the device (including any attached flash memory cards, such as secure digital (SD) and compact flash).

UE4.2.3

There should be documented standards / procedures covering the acceptable use of hand-held devices, which cover:

a) a specification of the types of device permitted (eg the manufacturer and make of the device; and features to be implemented such as complex passwords and device encryption)
b) restrictions on use (eg prohibiting personal use and sharing of hand-held devices with other staff and external individuals, or only permitting storage of non-sensitive information)
c) the rights of the organisation regarding ownership of information stored on hand-held devices (eg all information stored on a hand-held device remains the property of the organisation)
d) the right of the organisation to recover information stored on hand-held devices.

Section UE4.3 Portable storage devices

Principle The use of portable storage devices in the end user environment should be approved, access to them restricted, and information stored on them protected.

Objective To ensure that important information stored on portable storage devices is protected from unauthorised disclosure.

UE4.3.1

There should be documented standards / procedures covering the use of portable storage devices in the end user environment.

Portable storage devices include external hard disk drives, flash memory cards such as secure digital (SD) and compact flash, USB memory sticks, solid state storage and MP3 players with storage capacity for holding data.

Methods of connecting portable storage devices to computer equipment (eg laptop computers and desktop computers) include USB, FireWire and Bluetooth.

UE4.3.2

Standards / procedures should include:

a) the types of portable storage device permitted for storing business information (eg devices that are issued by the organisation)
b) restrictions on use of portable storage devices (eg prohibiting personal use and sharing of portable storage devices with other staff and external individuals, or only permitting storage of non-sensitive information)
c) the type of information that can be transferred to and from portable storage devices (eg restricted to non-classified information or encrypted files)
d) encryption of information stored on portable storage devices
e) the rights of the organisation regarding ownership of information stored on portable storage devices (eg all information stored on a portable storage device remains the property of the organisation)
f) the right of the organisation to recover information held on portable storage devices.

UE4.3.3

Portable storage devices should be protected by the use of:

a) authentication methods (eg by the use of UserID and password, biometrics such as fingerprint scan)
b) access restrictions
c) encryption techniques (eg using encryption software installed on the device, or using encryption software on the workstation, to which the portable storage device connects).

Area UE5
ELECTRONIC COMMUNICATIONS

Electronic communication in the end user environment should be subject to a range of controls which preserve the accuracy and confidentiality of information whilst also protecting the organisation from unintended consequences which may result from misuse of communications facilities. Accordingly, this area covers the approved use of electronic communications, end user behaviour when using electronic communication as well as the application of specific controls relating to e-mail; instant messaging; use of the Internet; Voice over IP (VoIP) networks; and wireless access.

Section UE5.1 General controls

Principle The use of electronic communications (eg e-mail, instant messaging, Internet access, Voice over IP or wireless access) should be supported by setting policy covering the types of communication permitted, and promoting user awareness of the security issues associated with their use.

Objective To ensure that the organisation's reputation is not damaged as a result of the transmission of inappropriate information, that the content of electronic communications is accurate, and that business activity is not disrupted by the introduction of malware.

UE5.1.1

Users with access to electronic communications (eg e-mail, instant messaging, Internet access, Voice over IP and wireless access) should be prohibited from:

a) opening attachments from unknown or untrusted sources
b) using offensive language
c) sending messages to unknown recipients
d) misusing electronic communication
e) using web communication applications (eg web-based e-mail and instant messaging, peer-to-peer file sharing and web logging (commonly referred to as blogging)).

UE5.1.2

Users should be made aware that:

a) the content of messages may be legally and contractually binding
b) electronic communication may be monitored.

UE5.1.3

Users should be made aware of the security features provided with electronic communications (eg digitally signing e-mails and encrypting instant messages).

Section UE5.2 E-mail

Principle Use of e-mail systems should be approved, and protected by a combination of policy, awareness, and procedural controls.

Objective To ensure that the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

UE5.2.1

The use of e-mail should be signed off by an appropriate business representative.

UE5.2.2

There should be documented standards / procedures for e-mail services (ie the application and supporting infrastructure), which include:

a) guidelines for business and personal use (eg prohibition of personal use)
b) the types of e-mail service permitted (eg corporate services such as Lotus Notes or Microsoft Exchange)
c) user guidelines for acceptable use (eg prohibition of the use of offensive statements)
d) details of any monitoring activities to be performed.

UE5.2.3

Users should be made aware that the:

a) content of e-mail messages may be legally and contractually binding
b) use of e-mail may be monitored.

UE5.2.4

The organisation should prohibit:

a) the use of web-based e-mail
b) automatic e-mail diversion to external e-mail addresses
c) unauthorised advertising
d) private encryption of e-mail or attachments
e) the opening of attachments from unknown or untrusted sources.

UE5.2.5

Personal use of business e-mail should be clearly labelled as personal and subject to the terms of a user agreement.

UE5.2.6

Users should be educated in how to protect the confidentiality and integrity of e-mail messages (eg by the use of encryption, digital certificates and digital signatures).

Section UE5.3 Instant messaging

Principle Use of instant messaging services should be approved, and protected by setting management policy, deploying instant messaging application controls and correctly configuring the security elements of an instant messaging infrastructure.

Objective To ensure that instant messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

UE5.3.1

Use of instant messaging should be signed off by an appropriate business representative.

UE5.3.2

There should be documented standards / procedures for instant messaging services (ie the application and supporting infrastructure), which include:

a) guidelines for business and personal use (eg prohibition of personal use)
b) the types of instant messaging service permitted (eg public services such as AOL, Google Talk, Windows Messenger and Yahoo!, or internal services such as Lotus Sametime, Windows Meeting Space, WebEx and Jabber)
c) user guidelines for acceptable use (eg prohibition of the use of offensive statements)
d) details of any monitoring activities to be performed.

UE5.3.3

Users should be made aware that the:

a) content of instant messages may be legally and contractually binding
b) use of instant messaging may be monitored.

UE5.3.4

The organisation should prohibit:

a) the use of web-based or personal instant messaging
b) private encryption of instant messaging or attachments
c) the opening of attachments from unknown or untrusted sources.

UE5.3.5

Personal use of business instant messaging should be:

a) clearly labelled as personal
b) subject to the terms of a user agreement.

UE5.3.6

Users should be educated in how to protect the confidentiality and integrity of instant messages (eg by the use of encryption, digital certificates and digital signatures).

Section UE5.4 Internet access

Principle Use of the Internet by end users should be approved, and protected by restricting the types of use permitted, deploying approved web browsers and promoting awareness of the risks associated with Internet access.

Objective To ensure that use of the Internet is restricted to legitimate business activity and that the risks associated with malicious code are minimised.

UE5.4.1

Use of the Internet in the end user environment should be signed off by an appropriate business representative.

UE5.4.2

There should be documented standards / procedures for Internet access (eg using a web browser such as Mozilla Firefox, Microsoft Internet Explorer, Opera or Apple Safari).

UE5.4.3

Standards / procedures for Internet access should include:

a) protection of workstations with access to the Internet (eg access control, malware protection, personal firewall and back-up)
b) the types of Internet service permitted
c) user guidelines for acceptable use (eg prohibition of the use of offensive statements and prohibition of personal use)
d) details of any monitoring activities to be performed.

UE5.4.4

Workstations that are capable of connecting to the Internet (eg using a web browser) should be protected by:

a) applying updates to applications and system software quickly and efficiently
b) restricting the downloading of mobile code (eg by excluding defined categories of executable software using a personal firewall, or equivalent)
c) using personal firewalls
d) installing host intrusion detection software (HIDS).

UE5.4.5

Users should be made aware that web browsing activity may be monitored.

UE5.4.6

The organisation should prohibit the use of non-corporate web browsers.

UE5.4.7

Personal web browsing of the Internet should be subject to the terms of a user agreement.

UE5.4.8

Users should be warned of the:

a) dangers posed by downloading mobile code (ie the possibility of downloading Java applets, MS ActiveX, JavaScript or VBScript, that have been written deliberately to perform unauthorised functions)
b) implications of accepting or rejecting 'cookies' (a small text file containing information that can be used to identify a user returning to a website)
c) opening of attachments downloaded from the Internet.

Section UE5.5 Voice over IP (VoIP) networks

Principle Voice over IP (VoIP) networks should be approved, and protected by a combination of general network and VoIP-specific controls.

Objective To ensure the availability of the VoIP network, protect the confidentiality and integrity of sensitive information in transit, and minimise the risk of misuse.

UE5.5.1

Use of Voice over IP (VoIP) should be signed off by an appropriate business representative.

UE5.5.2

There should be documented standards / procedures for VoIP services (ie the application and supporting infrastructure), which include:

a) guidelines for business and personal use (eg prohibition of personal use)
b) the types of VoIP service permitted (eg public services such as Skype and Google Talk, or internal services provided by vendors such as Avaya, Cisco and 3Com)
c) user guidelines for acceptable use (eg voice-mail, conferencing services and unified messaging)
d) details of any monitoring activities to be performed.

UE5.5.3

Users should be made aware of the:

a) information risks specific to VoIP-related software
b) standards / procedures for business and personal use (eg allowing personal use, but only outside of working hours)
c) types of VoIP services permitted (eg voice-mail, conferencing services and unified messaging)
d) user guidelines for acceptable use (eg prohibition of the use of offensive statements).

UE5.5.4

Personal use of corporate VoIP should be subject to the terms of a user agreement.

Section UE5.6 Wireless access

Principle Wireless access should be authorised, users authenticated and wireless traffic encrypted.

Objective To ensure that only authorised individuals can gain wireless access to the network, and minimise the risk of wireless transmissions being monitored, intercepted or modified.

UE5.6.1

Use of wireless access should be signed off by an appropriate business representative.

UE5.6.2

There should be documented standards / procedures for wireless access (ie software and supporting infrastructure), which include:

a) guidelines for business and personal use (eg prohibition of personal use)
b) the types of wireless access service permitted
c) user guidelines for acceptable use (eg prohibition of connecting personal or unapproved equipment, such as desktop computers, laptop computers, and hand-held devices)
d) details of any monitoring activities to be performed.

UE5.6.3

Wireless networks should be implemented in compliance with enterprise-wide standards / procedures for wireless access.

UE5.6.4

Users should be made aware of the:

a) types of wireless access permitted (eg only allowing connection to corporate wireless access points or only connecting to the corporate network using a VPN when working in a remote location)
b) threats associated with wireless access (eg monitoring of network traffic, cracking wireless encryption keys, interception and radio interference)
c) steps required to minimise the risks associated with wireless access (eg only enabling the wireless network interface card when required, using encryption such as WPA and WPA2, and protecting authentication details such as encryption keys, passwords and tokens).

Area UE6
ENVIRONMENT MANAGEMENT

End user environments are important to the success of the organisation, therefore security arrangements within the end user environment should reflect those made on an enterprise-wide basis. Accordingly, this area covers the protection of personally identifiable information; information security incident management; back-up of important information and software; physical protection of the end user environment; and business continuity.

Section UE6.1 Information privacy

Principle Approved methods for handling personally identifiable information should be established and applied.

Objective To prevent information about individuals being used in an inappropriate manner, and to ensure compliance with legal and regulatory requirements for information privacy.

UE6.1.1

There should be documented standards / procedures for dealing with information privacy, which cover the:

a) acceptable use of personally identifiable information (ie information that can be used to identify an individual person)
b) rights of the individual about whom personally identifiable information is held.

UE6.1.2

The individual responsible for managing the end user environment should be aware of:

a) the location of personally identifiable information held about individuals (eg application and database servers, workstations, hand-held devices and portable storage devices)
b) how and when personally identifiable information is used.

UE6.1.3

Where personally identifiable information is stored or processed, there should be methods in place to ensure that it is:

a) adequate, relevant and not excessive for the purposes for which it was collected
b) accurate (eg by ensuring information is recorded correctly and kept up-to-date)
c) kept confidential
d) processed fairly and legally
e) used only for specified, explicit and legitimate purposes
f) held in a format that permits identification of individuals for no longer than is necessary
g) only provided to third parties that can demonstrate compliance with legal and regulatory requirements for handling personally identifiable information
h) retrievable in the event of a request for access.

UE6.1.4

Personally identifiable information should be handled in accordance with relevant legislation (eg the EU Directive on Data Protection, the US Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry (PCI) Data Security Standard).

Section UE6.2 Information security incident management

Principle Information security incidents should be identified, responded to, recovered from, and followed up using an information security incident management process.

Objective To identify and resolve information security incidents effectively, minimise their business impact and reduce the risk of similar information security incidents occurring.

UE6.2.1

There should be a documented information security incident management process that applies to the end user environment, which includes:

a) identifying information security incidents
b) responding to information security incidents
c) recovering from information security incidents
d) following up information security incidents.

UE6.2.2

Information security incidents should be:

a) reported to a predetermined contact (eg a helpdesk, telephone hot line or specialist IT team / department)
b) recorded in a log, or equivalent (eg using an automated information security incident management system)
c) categorised and classified (eg according to their severity and type).

UE6.2.3

The business impact of serious information security incidents should be assessed by an information security specialist.

UE6.2.4

The response to information security incidents should include:

a) analysing available information (eg application and system event logs)
b) handling necessary evidence (eg labelling it and storing it in a safe location to prevent unauthorised tampering)
c) investigating the cause of information security incidents (eg with assistance from the information security incident management team)
d) containing and eradicating the information security incident (eg by making changes to access control or terminating network connections).

UE6.2.5

The recovery of information security incidents should involve:

a) rebuilding applications (and supporting IT facilities) to a previously known secure state (ie the same state they were in before the information security incident occurred)
b) restoring information that has not been compromised by the information security incident
c) closure of the information security incident.

(continued on the next page)

Section UE6.2 Information security incident management (continued)

UE6.2.6

Following recovery from information security incidents:

a) reviews should be performed to determine the cause (eg by performing a root cause analysis) and effect of the information security incident and corresponding recovery actions
b) forensic investigations should be performed if required (eg for legal purposes or serious information security incidents, such as fraud)
c) existing security controls should be examined to determine their adequacy
d) corrective actions should be undertaken to minimise risk of similar incidents occurring
e) details of the information security incident should be documented in a post-incident report.

Section UE6.3 Back-up

Principle Back-ups of essential information, applications and software used in the end user environment should be performed on a regular basis, according to a defined cycle.

Objective To ensure that, in the event of an emergency, essential information or software required in the end user environment can be restored within critical timescales.

UE6.3.1

Back-ups of essential information, applications and software in the end user environment should be performed, which include information held on:

a) desktop computers (eg personal computers that are typically located in a fixed location such as an office)
b) laptop computers (eg portable personal computers)
c) hand-held devices (eg Personal Digital Assistants (PDAs), WAP-based mobile phones and smartphones)
d) portable storage devices (eg external hard disk drives, flash memory cards secure digital (SD) and compact flash, USB memory sticks, solid state storage and MP3 players with storage capacity for holding data).

UE6.3.2

Back-ups of information, applications and software should be performed frequently enough to ensure they can be restored within a critical timescale (ie the timescale beyond which an outage is unacceptable to the organisation).

UE6.3.3

The security of back-ups should be strengthened by the use of a back-up management package.

UE6.3.4

Back-ups should be verified to ensure that backed-up software and information can be restored successfully.

UE6.3.5

Back-ups should be protected from loss, damage and unauthorised access, by:

a) storing them in a computer media fireproof safe on-site, to enable important information to be restored quickly
b) keeping copies off-site, to enable the application to be restored using alternative facilities in the event of a disaster
c) restricting access to authorised staff (eg through the use of access control software, physical locks and keys).

Section UE6.4 Physical and environmental protection

Principle The end user environment (and sensitive material stored within it) should be subject to a range of physical and environmental controls.

Objective To restrict physical access to authorised individuals and ensure that IT facilities processing critical information are available when required.

UE6.4.1

There should be documented standards / procedures for the provision of physical and environmental protection over the end user environment.

UE6.4.2

The standards / procedures should cover the protection of:

a) buildings against unauthorised physical access (eg by using locks, security guards and video surveillance)
b) important papers and removable storage media against theft or copying (eg by locking them away and restricting access)
c) equipment (eg wireless access points, facsimile machines and printers) against theft (eg by being locked away when not in use or by using specialised locks).

UE6.4.3

The end user environment should be protected against unauthorised physical access by:

a) providing locks, bolts or equivalent on vulnerable doors and windows
b) employing security guards.

UE6.4.4

Sensitive material (eg access tokens, blank cheques, print-outs of personal information and removable storage media containing PIN data) should be:

a) stored in a physically secure location (eg a fire-proof safe) and in accordance with manufacturers specifications
b) protected in transit (eg by recording authorised recipients, clearly marking all material and confirming receipt)
c) monitored by recording its issue and use
d) disposed of in a secure manner (eg erasure, incineration or shredding)
e) protected from unauthorised disclosure (eg by using encrypted facsimile or keeping relevant printers / photocopiers in locked areas).

UE6.4.5

Important papers and removable storage media (eg external hard disk drives, rewritable CDs / DVDs and USB memory sticks) should be protected against theft or copying by:

a) storing sensitive physical material in locked cabinets (or similar) when not in use (eg by enforcing a 'clear desk' policy)
b) restricting physical access to important post and facsimile points.

UE6.4.6

Staff that may be subject to intimidation (eg engineers, bank tellers or pharmacists) should be protected by the:

a) provision of 'duress alarms' (or equivalent)
b) establishment of a process for responding to emergency situations.

(continued on the next page)

Section UE6.4 Physical and environmental protection (continued)

UE6.4.7

The end user environment should be protected from natural hazards (eg flood and fire) by the use of early warning alarms, fire detection and fire suppression systems, and easily accessible hand-held fire extinguishers.

UE6.4.8

The power supply to systems in the end user environment should be protected by uninterruptible power supplies (UPS).

UE6.4.9

Back-up generators should be available to provide an alternative source of power in the event of extended power failure.

Section UE6.5 Business continuity

Principle A business continuity plan should be established, supported by contingency arrangements, and tested regularly.

Objective To enable the business processes associated with the end user environment to continue in the event of a disaster.

UE6.5.1

There should be an individual in the end user environment that is responsible for managing business continuity arrangements.

UE6.5.2

There should be a documented business continuity plan (or equivalent) that applies to the end user environment, which is based on, or aligned with, an enterprise-wide business continuity plan.

UE6.5.3

The business continuity plan should specify:

a) recovery tasks to be carried out, in priority order
b) responsibilities of individuals, with nominated deputies
c) arrangements for the safe storage of plans, and their retrieval in case of emergency
d) testing of information security arrangements (eg rebuild and configuration of firewalls, malware protection software and intrusion detection mechanisms).

UE6.5.4

Individuals within the end user environment should be made aware of the responsibilities assigned to them in the business continuity plan.

UE6.5.5

The business continuity plan should cover the reconfiguring or restoring of information security systems used in the end user environment.

UE6.5.6

There should be business continuity arrangements (eg a separate processing facility ready for immediate use, reciprocal arrangements with another organisation or a contract with a specialist business continuity arrangements provider) in case of a disaster or emergency.

UE6.5.7

Business continuity arrangements should cover the prolonged unavailability of:

a) key individuals (eg due to illness, injury, vacation or travel)
b) important information (eg due to loss or corruption of business information, documentation, and back-up files)
c) system or application software (eg due to human error or malfunction of software)
d) computer equipment (eg due to malfunction of hardware, or human error)
e) network equipment, cabling or links (eg due to loss of voice, data or other communications systems)
f) office accommodation, buildings, machine rooms, power, communications and other vital services (eg due to damage following fire, flood, or similar incidents)
g) access to systems or buildings (eg due to police, military or terrorist action, natural disaster or withdrawal of transport services)
h) essential services (eg loss of electricity, gas or water supplies).

(continued on the next page)

Section UE6.5 Business continuity (continued)

UE6.5.8

Business continuity arrangements should be checked to ensure that they will work within critical timescales (ie the timescale beyond which an outage is unacceptable to the organisation) by carrying out:

a) tests of alternative processing arrangements (eg attempting to run the application from a back-up site)
b) realistic simulations (eg involving users, information security specialists and IT staff).

Index

A

Abuse / misuse

SM3.4.4, CB5.3.3, CI4.1.4, CI5.4.4, NW2.2.4, NW4.4.4, SD3.5.4, UE5.1.1

Acceptable use

SM4.2.3, SM6.8.1, UE4.2.3, UE5.2.2, UE5.3.2, UE5.4.3, UE5.5.2-3, UE5.6.2, UE6.1.1

Acceptance

Criteria

SD6.1.1

Testing

CI2.1.3, **SD5.2**, SD1.4.2, SD2.3.3

Access

Administrator,

NW1.2.2

Agreements

NW1.5.2

Arrangements

SM4.4.1-6, CB4.1.3, CB4.1.6, CB6.1.1, CI4.1.1-4, NW1.5.6

Building,

SM4.5.2-3, SM5.5.3, CB2.5.6, CI6.2.2, NW3.6.2, UE6.4.2, UE6.5.7

Control

SM4.4.1, SM5.6.5, SM6.2.3, SM6.4.1, SM6.4.3, **CB3.1**, CB2.4.5, CB3.2.1, CB3.3.1, CB3.3.3, CB3.4.5, CB4.3.5, CB4.4.4, CB6.1.1, CB6.3.3, **CI4.1**, CI1.2.3, CI2.2.2, CI2.4.1, CI2.4.3, CI3.4.5, CI3.6.5, CI5.5.3, NW2.1.2-3, NW2.4.5, NW3.3.5, NW3.7.2, SD1.4.3-4, SD3.1.6, SD4.3.2, SD4.5.4, SD5.2.4, **UE2.1**, UE1.2.7, UE1.3.2, UE3.2.5, UE3.3.6, UE4.1.2, UE4.2.2, UE5.4.3, UE6.2.4, UE6.3.5

Control logs

CB3.1.6, CB3.1.7, CI2.2.2, NW2.3.7, SD1.4.3

Control mechanisms

SM6.2.3, SM6.4.1, SM6.4.3, CB3.1.5, CB3.3.1, CB3.3.3, CB6.1.1, CB6.3.3, CI2.4.1, CI2.4.3, NW2.1.2, NW3.5.1, SD1.4.4, UE1.2.7, UE2.1.3, UE4.1.2, UE4.2.2

Control lists

CB4.3.5, UE3.2.5, UE3.3.6

Control policies

CI4.1.4, NW2.1.1, NW2.2.2, NW5.1.1, NW5.4.1

Control software

CB4.4.4, SD1.4.3, UE6.3.5

Control testing

SD5.2.4

External,

CB4.3.3-5, NW2.3.1, NW2.3.7

Physical,

SM4.5.4, CI2.8.1-2, CI2.8.7-8, NW3.4.1, SD1.4.4, UE6.4.2-3, UE6.4.5

Privileges

SM1.3.4, SM3.2.2-3, SM4.1.5-6, SM4.4.4, SM4.4.6, SM6.5.3-4, CB2.1.3, CB2.2.6, CB3.1.5, **CI4.3**, CI4.1.2, CI4.1.4, CI4.2.2, CI4.2.4, CI4.5.3, CI4.5.5, NW3.7.1, UE1.1.3, UE1.1.10, UE1.3.3, UE2.1.5-6

Rights

See Access Privileges

Third party,

SM3.4.4, SM6.5.1, SM6.5.5-6, CB5.3.3, CB5.4.3, CB6.1.1, CB6.1.2, CB6.1.3, CB6.1.4, CB6.1.5, CI5.4.4, NW4.4.4, SD3.5.4

Unauthorised,

SM4.4.2-3, SM4.5.2-3, SM5.3.3, SM5.5.4, CB4.4.4, CB6.2.3, CI2.3.4, CI3.2.6, NW2.1.3, NW3.5.4, NW5.1.1, SD1.4.4, SD4.5.4, SD4.6.7, UE6.3.5, UE6.4.2-3

Wireless,

CI2.8.2, CI2.8.6, NW2.4.1-7, UE5.1.1, UE5.6.1-4, UE6.4.2

Accountability

SM6.5.3, CB3.1.5, CI4.1.2, NW2.1.3, SD1.1.1, UE2.1.4, UE6.1.4

Accounting

CI3.1.4, NW2.3.5, UE1.2.5, UE1.3.1

Packages

UE1.2.5, UE1.3.1

Acquisition

SM4.3.1-2, SM4.3.4, SM7.2.6, NW1.3.3, SD2.3.3, SD3.2.3, SD3.3.3, SD3.4.3, **SD4.4**, SD4.1.4

ActiveX

SM5.1.1, SM5.2.8, SM6.4.1, CB3.3.1, CB3.3.3, CB3.3.5, CI1.2.3, CI2.4.1, CI2.4.3, CI2.4.5, SD1.4.3, UE5.4.8

Application

Business,

SM2.1.3, SM2.3.2, SM3.1.5, SM3.3.1, SM4.1.4, SM4.4.2, SM4.7.5, SM5.6.1, SM7.1.1, CB2.6.1, CB3.1.2, CB3.3.1, CB6.4.2, CI2.1.4, CI3.5.2, CI3.6.1, CI4.5.5, CI5.4.2-3, CI5.5.2, CI6.1.4, NW4.4.2-3, NW4.5.2, SD4.6.3, UE1.2.5, UE1.3.1-2, UE2.1.1, UE2.1.3, UE2.2.1, UE2.3.1, UE2.3-6

Communication,

UE5.1.1

Controls

CB2.2, SD2.3.3, **SD4.2**, UE1.2.7, UE3.4.6

Desktop,

SM4.3.6, CI1.3.2, **UE3.4**, UE1.2.5, UE1.2.7, UE1.3.1, UE1.3.2, UE2.3.7, UE3.1.1, UE3.1.2, UE3.1.3, UE3.1.4

Development

CI1.3.2, **UE3.2-4**, UE1.3.1, UE3.1.1-2, UE3.2.1-2, UE3.3.1-2, UE3.4.1-2, UE3.4.7, UE3.4.10

Firewall

See Firewall

Management

CB5.4.3

Owner(s)
CB2.1.1-2, CB2.4.4, CB3.1.5, CB4.1.2, CB5.1.1, CB5.1.3, CB5.3.7, CB5.4.4, CB5.4.6, CI1.2.1-2, CI1.4.8, CI4.1.2, CI4.1.4, NW1.5.1, NW3.1.7, NW3.3.4, NW4.4.3, SD6.1.2

Packages / software
SM4.7.4, SD4.4.1, SD5.1.3, UE6.5.7

Programming Interface (API)
SM4.1.2, SM4.1.6, CB6.4.3, SD4.6.4, SD4.6.11

Specialist
CB2.4.4, UE3.4.7

Application proxy firewall
See Firewall

Archiving
SM4.3.1, SM4.3.8, CI1.2.3, CI1.4.2, CI3.2.3, CI3.2.5, SD1.4.3, SD6.2.2

Asset management / register
SM4.3, **CI1.3**, CI3.6.2

Audit / review
SM7.1, SM2.2.3, SM3.2.2, **CB5.4**, CB6.1.3, **CI5.5**, NW2.3.5, NW3.2.5, **NW4.5**, **SD2.3**

Audit trails
NW1.1.5, NW1.2.2

Authentication

Biometric,
SM2.2.4, UE4.3.3

Details
CB3.1.3, CB3.1.8, CB3.2.4, CI4.3.5, CI4.4.4, SD1.4.3, UE5.6.4

Device,
NW2.4.5

Hardware
SM1.3.7

Information
SM4.4.5, UE2.1.1

Mechanisms
See Authentication Methods

Methods
CB3.1.2, CB4.1.3, UE2.1.1, UE2.1.3, UE4.3.3

Mutual,
CB6.4.3, SD4.6.4

Of connection(s)
NW2.3.7, NW2.4.9

Services
SM2.2.2, SM4.1.6

Sharing of,
CB3.1.3

Strong,
SM3.4.7, SM4.4.1, SM 6.1.1, SM6.2.3, CB3.1.2, CB4.3.3, CB5.3.6, CB6.2.1, CB6.3.3, CI4.1.4, CI4.5.1, CI4.5.5, CI5.4.7, NW2.1.2, SD3.5.7, UE2.1.3

System
NW2.3.7

Token-based,
CI4.1.4

User,
CI4.5.2, CI4.5.3, NW2.4.5, NW5.1.1

Authorisation
SM1.2.7, SM6.4.1, CB3.1.5, CB6.4.6, **CI4.2**, CI2.3.3, CI2.8.8, CI3.5.5, CI4.3.2, SD5.2.6

Authorised individuals / staff
SM6.2.3, CB2.3.3, CB3.2.1, CB4.4.4, CB6.2.1, CB6.4.6, CI2.1.2, CI2.1.4, CI2.8.1, CI3.2.6, CI3.3.3, NW1.4.3, NW2.1.3, NW2.2.2, NW3.1.5, NW3.2.3, NW3.4.1, NW3.5.4, NW5.3.2, SD4.6.7, UE2.3.4, UE3.2.5, UE3.3.6, UE6.3.5

Authorised personnel
See Authorised individuals

Authorised users
CB2.1.3, CB2.2.6, CB3.2.3, CI2.1.2, CI4.2.3-4, CI4.4.3, NW2.4.2, SD5.2.2, UE1.1.3, UE1.1.10, UE2.2.3

Automated software tools
CB2.2.2, CB2.2.7, CB5.4.4, CI1.4.5, CI2.2.8, CI5.5.4, NW4.5.4, SD2.3.4, SD4.2.3, SD4.5.4, SD5.1.6, UE3.4.9

Availability
SM1.2.3, SM2.4.3, SM3.1.1, SM3.4.4, SM4.6.1, SM4.7.4, SM6.3.3, SM6.7.4, CB3.4.3, CB5.2.1, CB5.3.3, CI1.4.4, CI2.2.3, CI5.2.3, CI5.3.1, CI5.4.4, NW1.3.4, NW4.2.3, NW4.3.1, NW4.4.4, SD1.3.2, SD2.2.3, SD3.1.3, SD3.4.1-5, SD3.5.4, SD4.1.1, SD4.1.3, SD4.2.1, SD4.3.1, SD4.3.5, UE1.2.3, UE1.5.1, UE3.4.2

Requirements
CB1.3, CB6.1.4, **SD3.4**, SD2.3.3, SD3.4.4, SD3.4.5

Awareness

Material
SM2.4.2, CB3.4.2, CI5.2.2, NW4.2.2, SD2.2.2, UE1.2.2

Programmes
SM2.2.2, SM2.4.1, SM7.1.1, CB3.4.2, CI5.2.2, NW4.2.2, SD2.2.2, SD2.2.6, UE1.2.2

B

Back doors
SD5.2.3

Back-office system
CB6.4.3, CB6.4.4, SD4.6.4, SD4.6.5

Back-out
CB2.3.3, CI3.3.3, NW3.2.3

Back-up

SM6.4.5, **CB4.4**, CB2.5.6-7, CB4.4.1-4, CB6.1.4, CB6.2.1, CB6.3.3, **CI3.2**, CI1.2.3, CI2.1.2, CI2.2.2, CI2.4.3, CI2.5.5, CI4.1.3, CI6.1.6, CI6.2.2, **NW3.5**, SD4.3.5, **UE6.3**, UE3.2.5, UE3.3.6, UE6.5.7-8

Cycles

CI3.2.2, CI3.2.5

Generators

CB4.2.5, CI2.7.2-3, NW3.6.4, UE6.4.9

Processes

CI3.2.2-4, UE5.4.3, UE6.3.4

Protection of,

CB4.4.4, CI3.2.6, NW3.5.4, UE6.3.5

Software

SM6.4.3, SM4.6.7, CB3.3.3, CB4.4.2, CI2.4.3, CI3.2.4, NW3.5.2, UE1.2.7, UE4.1.2, UE6.3.3

Base code

SD4.5.2, SD4.5.5-6

Basel II

SM2.2.4, SM3.4.6, CB5.3.6, CB6.1.1, CI5.4.7, NW4.4.7, SD3.5.7

Biometrics

SM4.4.4, CB3.1.2, CB4.3.3, CI4.1.4, UE2.1.3, UE4.3.3

Bluetooth

SM2.2.4, UE4.3.1

Bottlenecks / overloads

SM6.3.2, CI1.4.1, CI1.4.3, NW2.1.2, NW3.1.1-2, SD2.2.3, SD2.2.6

Buffer overflows / overrun

SM5.3.8, CI1.4.6, NW3.1.4, SD4.5.7

Business

Application

SM2.1.3, SM2.3.2, SM3.1.5, SM3.3.1, SM4.1.4, SM4.4.2, SM4.7.5, SM5.6.1, SM7.1.1, CB2.6.1, CB3.1.2, CB3.3.1, CB6.4.2, CI2.1.4, CI3.5.2, CI3.6.1, CI4.5.5, CI5.4.2-3, CI5.5.2, CI6.1.4, NW4.4.2-3, NW4.5.2, SD4.6.3, UE1.2.5, UE1.3.1-2, UE2.1.1, UE2.1.3, UE2.2.1, UE2.3.1, UE2.3.5-6

Impact

SM3.1.1, SM3.4.4, SM3.4.6, SM4.6.4, SM5.3.8, SM5.6.4, SM7.2.2-3, CB2.3.3, CB2.4.4, CB5.2.2, CB5.3.3, CB5.3.5, CI2.3.5-6, CI3.3.3, CI3.4.4, CI3.6.4, CI5.3.2, CI5.4.4, CI5.4.6, NW3.2.3, NW3.3.4, NW4.3.2, NW4.4.4, NW4.4.6, SD3.5.4, SD3.5.6, UE1.5.2, UE2.3.4, UE2.3.7, UE6.2.3

Information

SM1.2.7, SM4.7.4, SM7.1.3, CB2.1.3, CB2.3.1, CB2.5.6, CB3.4.5, CB4.4.1, CB5.4.5, CI3.1.2, CI3.2.1, CI3.3.1, CI4.1.3, CI5.2.5, CI5.5.5, CI6.2.2, NW3.5.1, NW4.2.5, NW4.5.5, SD1.4.4, SD2.2.5, SD2.3.5, SD4.3.5, SD5.2.6, SD6.1.2, UE1.1.3, UE1.2.4, UE2.3.2, UE4.3.2, UE6.5.7

Integrity

SM6.3.6

Manager

SM2.2.5, SM6.1.4, SM6.6.1, CB2.1.1, CB2.3.5, CI3.3.5, NW3.2.5, UE1.1.1, UE2.3.6

Owner

SM2.1.3, SM3.1.3, SM3.3.3, SM3.5.1, SM3.5.5, SM6.5.5, SM6.6.2, SM6.7.3, CB5.2.4, CB5.3.2, CI1.2.2, CI2.1.4, CI3.2.3, CI3.5.2, CI5.4.3, SD1.1.1, SD2.1.3, SD2.3.5, SD3.1.7, SD3.5.3, SD3.5.8

Representative

SM2.4.2, SM3.4.2, SM4.3.4, SM6.4.1, CB2.3.3-4, CB2.5.2, CB3.2.5, CB4.1.4, CB4.3.1, CB5.3.7, CB5.4.5, CB6.1.2 , CI1.4.4, CI3.3.3-4, CI3.5.3, CI4.3.1, CI4.3.3, CI5.3.4, CI5.4.8, NW1.1.4, NW3.2.3-4, NW4.3.4, NW4.4.8, SD4.4.6, SD5.1.8, SD6.1.2, SD6.3.3, UE1.5.4, UE2.3.4-5, UE2.3.9, UE3.1.4, UE3.4.3, UE3.4.5, UE5.2.1, UE5.3.1, UE5.4.1, UE5.5.1, UE5.6.1

Requirements

SM3.2.2, SM6.6.4, CB1.3.5, CB4.4.1, CI2.2.2, CI3.2.1, CI4.1.4, NW3.5.1, SD1.2.2, SD1.3.2, SD2.3.3, SD3.1.1-7, SD3.2.1, SD3.3.1, SD3.4.1, SD3.4.6, SD5.1.5, SD6.3.2

Risks

SM6.5.1-2, SM7.2.7, CB5.4.2, CI5.5.2, NW4.5.2, SD2.3.2

Trends

SM2.2.4

Users

SM2.5.2, CB2.1.3, CB4.1.3, CI1.2.3, CI1.4.4, CI4.1.3, CI4.3.1, CI6.1.5, CI6.2.3, CI6.3.2, SD5.2.3, UE1.1.3

Business continuity

SM4.7, **CB2.5**, **UE6.5**

Arrangements

SM4.7.3-7, SM6.7.5, CB2.5.5-7, CI5.5.3, CI6.1.6, NW5.2.6, UE6.5.1, UE6.5.6-8

Plans

SM2.5.4, SM4.7.1-2, CB2.5.2-4, CI3.2.3, CI6.1.2, NW3.6.1, NW5.2.6, UE6.5.2-5

Responsibility

SM4.7.7, CB2.5.1, CB2.5.4, UE6.5.1, UE6.5.3-4

C

Cabling

CB2.5.6, CI2.7.1, NW1.4.1-2, NW1.4.4, NW3.4.3, NW3.6.2, NW4.3.3, NW5.1.3, NW5.2.3, NW5.2.5, UE6.5.7

Capacity

SM6.6.5, NW1.3.3, NW3.1.2, NW5.2.1, SD4.3.5, SD5.1.5

Planning

CI1.4.3, NW3.1.2

Requirements

CB4.1.1-2, CI1.2.1-2, NW1.5.1-2, NW5.3.3, SD3.1.2, SD6.1.2

CCTV

See Closed-circuit television (CCTV)

Certification Authority (CA)
SM6.2.3, CB6.3.1, CB6.3.3

CGI
See Common Gateway Interface (CGI)

Chain letters
SM6.3.1, SM6.3.4

Change management
SM4.1.5, SM6.2.3, **CB2.3**, **CI3.3**, **NW3.2**, **UE2.3**

Discipline
See Change management process

Practices
SM4.7.1, SD5.2.2

Process
SM6.7.5, CB2.3.1-6, CB4.1.3, CB6.1.3, CB6.1.5, CB6.3.3, CI1.2.3, CI2.5.5, CI3.3.1-5, CI3.5.5, NW1.5.3, NW2.1.1, NW3.2.1-6, NW3.6.3, NW5.1.1, SD4.3.4, SD5.2.2, UE2.3.1-3, UE2.3.7, UE2.3.9, UE3.4.11

System
SM4.4.5

Change requests
CB2.3.3, CI3.3.3, NW3.2.3, UE2.3.4

'Clear desk' policy
SM1.2.6, SM4.5.4, CI2.8.2, UE6.4.5

Closed-circuit television (CCTV)
SM4.5.3, SM5.5.3, CI2.8.7

Common Criteria
SM4.3.3, CI2.5.4, SD4.4.4

Common gateway interface (CGI)
CI2.1.4, SD4.6.10-11

Communications equipment / facilities
CI6.2.2, NW1.3.2-3, NW1.4.1-2, NW1.4.4, NW3.2.1, NW3.4.1, NW3.6.2, NW3.6.4, SD4.4.1,
See also Network equipment

Communication(s) services
SM4.7.4, CB2.5.6, CI2.3.2, NW1.3.3, NW1.4.1-2, NW3.2.1, SD5.1.3, UE6.5.7

Compliance

Assesment of,
SM1.2.5, SM4.2.7

Process
SM3.5.2-4

Programme
SM4.2.3, SM4.2.7

Requirements
SM3.4.5, SM3.4.7, SM3.5.5, SM4.2.4, SM5.5.2, SM6.4.5, SM6.5.2, SM6.7.4, SM7.2.7, CB3.1.7, CB5.3.1, CB5.3.4, CB5.3.6, CI3.2.3, CI5.4.1, CI5.4.5, CI5.4.7, NW1.2.2, NW1.3.3, NW4.4.5, NW4.4.7, SD1.1.2, SD1.2.7, SD1.3.1, SD3.1.4, SD3.5.1, SD3.5.5, SD3.5.7, SD4.1.1, SD4.5.2, UE5.6.3, UE6.1.3

Review
SM3.5.5, SM3.5.6

Software Licensing
SM1.2.3, SM3.5.5

With policy
SM1.2.5-6, SM2.4.3, CB3.4.1, CB3.4.3, CB5.2.1, CB6.1.2, CI5.2.1, CI5.2.3, CI5.3.1, CI6.1.1, NW4.2.1, NW4.2.3, NW4.3.1, SD1.2.2, SD2.2.1, SD2.2.3, SD4.5.4, UE1.2.1, UE1.2.3, UE1.5.2, UE5.6.3

Computer Emergency Response Team (CERT) alerts
CI2.3.6, NW1.3.5

Computer media

Handling,
SM1.2.6, SM4.5.2, SM4.5.4, SM5.5.34, **CI3.1**

Confidential information
SM6.1.2, SM6.4.5, CB1.1.1-4, CB3.4.4, CI5.2.4, NW1.5.3, NW4.2.4, SD2.2.4, SD3.2.2-5, UE1.2.6

Confidentiality
SM1.2.3, SM1.3.2, SM2.4.3, SM3.1.1, SM3.4.4, SM4.6.1, SM6.1.1-2, SM6.7.4, CB2.6.1, CB3.4.3, CB5.2.1-2, CB5.3.3, CB6.1.4, CB6.2.1, CI5.2.3, CI5.3.1-2, CI5.4.4, NW4.2.3, NW4.3.1-2, NW4.4.4, SD1.3.2, SD2.2.3, SD3.1.3-4, SD3.2.1, SD3.5.4, SD4.1.1, SD4.1.3, SD4.2.1, SD4.3.1, SD4.3.3, UE1.1.6, UE1.2.3, UE1.5.1-2, UE2.1.1, UE3.4.2, UE5.2.6, UE5.3.6

Agreements
SM1.3.3, CI1.1.3, NW1.1.3, UE1.1.9

of passwords
CI4.5.2

Requirements
CB1.1, **SD3.2**, SD2.3.3

Configuring network devices
NW2.1

Contingency

Arrangements
SM6.7.8, **CI6.2**, CI6.3.1-4

Plans
SM6.2.4, CB6.3.4, **CI6.1**, CI6.3.1-4, NW3.6.1, NW5.2.6, SD3.1.4, SD4.3.5, SD5.2.4, SD6.1.3

Continuity of service
CB4.1.3, CI1.2.3, NW1.5.3, NW3.6.1, NW5.2.6

Contract(s)
SM1.3.1, SM2.2.3, SM3.1.2, SM6.5.1-2, SM4.7.3, SM6.5.5-6, SM6.7.4, CB1.1.1, CB1.2.1, CB1.3.1, CB2.5.5, CB4.1.1, CB5.2.3, CI1.2.1, CI5.3.3, CI6.1.6, NW1.5.1, NW4.3.3, NW5.2.3, SD1.4.5, SD3.2.2, SD3.2.4, SD3.3.2, SD3.3.4, SD3.4.2, SD3.4.4, UE1.1.7, UE1.2.5, UE1.5.3, UE6.5.6

Contractor(s)
SM1.3.3, SM1.3.5, SM3.3.2, CI1.1.3, NW1.1.3, NW3.4.1, UE1.1.9, UE1.2.1

Contractual

Conditions
SM6.3.6, SM6.5.2, CI4.3.3

Obligations
SM1.2.3-4, CI3.2.3, CI4.1.2, NW3.6.3, SD3.1.4, SD3.2.2, SD3.3.2, SD3.4.2, UE5.1.2, UE5.2.3, UE5.3.3

Terms
SM3.4.5, SM4.3.2, SM6.3.6, CI2.5.3, SD3.5.5, SD4.4.2-3

Control panels
CI2.3.2

Control weaknesses
SM3.4.4, CB5.3.3, CI5.4.4, NW4.4.4, SD3.5.4

Cookies
SM6.4.7, CB3.3.5, CI2.4.5, SD4.6.9, UE5.4.8

Copyright
SM1.3.2, SM6.5.2, CB6.1.3, UE1.1.6

Copying
SM3.1.4, NW2.1.2, SD1.4.5, SD4.5.6

Unauthorised,
SM1.2.7, SM4.5.2, SM4.5.4, CB3.4.4, CI5.2.4, NW4.2.4, SD2.2.4, UE1.2.6, UE6.4.2, UE6.4.5

Corporate governance
SM1.1.1, SM3.5.2

Corrective actions
CB2.4.7, CI3.4.7, NW3.3.7, UE6.2.6

Critical equipment
CB4.2.4, CI2.7.2, CI2.8.5, CI2.8.7, NW1.2.2, NW1.3.2-4, NW3.6.2, NW3.6.4, NW5.2.4

Critical timescales
SM4.7.6, SM5.4.4, CB1.3.5, CB2.5.7, CB4.4.3, CI1.2.2, CI3.2.5, CI6.1.4, CI6.3.2, NW1.3.3, NW1.5.2, NW3.5.3, SD3.4.6, UE6.3.2, UE6.5.8

Criticality
SM7.2.3, CB6.1.1, CI1.2.2

Cryptographic

Algorithms
SM6.1.2

Controls
CI1.2.3, SD4.3.3

Key management
SM6.1.2-3, SM6.2.1, **CB6.2**, CB5.4.3, CB6.1.4, CB6.3.1

Services
SM2.2.2, SM4.1.6

Solutions
SM6.1

Techniques
SM4.1.7, CI1.2.3

Cryptography
SM2.2.3, SM6.1.1-2, SM6.1.4, CB2.6.1

Customer(s) / client(s)
SM4.2.7, SM6.6.5, CB1.1.3, CB1.2.3, CB1.3.3, CB2.1.3, CB2.2.3, CB2.3.5-6, CB3.4.4, CB5.2.3-4, CI5.3.3, NW4.3.3, SD3.2.3-4, SD3.3.3-4, SD3.4.3-4, SD4.2.2, SD4.5.8, UE1.1.3, UE1.2.5-6, UE1.3.1, UE1.5.3, UE2.3,6, UE3.1.2

D

Data protection
SM1.3.2

EU directive on,
SM4.2.5-6, UE6.1.4

Legislation
SM6.7.5, UE1.1.6

Manager
SM4.2.1

Data privacy
SM2.2.4, SM3.4.7, SM3.5.2, SM6.4.5, SM6.5.2

Requirements
CB5.3.6, CI5.4.7, NW4.4.7, SD3.5.7

Data storage
CB4.2.3, CI2.5.2

Media
CI2.5.5, CI3.1.1-2, CI3.1.5-6

Data subject
SM4.2.5

Demilitarised Zone (DMZ)
SM5.2.8, CB6.4.2, NW1.2.2, SD4.6.3

Denial of service
SM3.4.4, SM5.3.8, CB5.3.3, CI1.4.6, CI5.4.4, NW2.2.4, NW3.1.4, NW4.4.4, SD3.5.4

Design / build
SM2.5.3, SM3.4.7, SM4.1.2, SM4.1.4-5, SM6.4.1, CB2.2.5, CB3.3.1, CB5.3.6, CI2.1.1-2, CI2.4.1, CI5.4.7, NW1.1.3, NW1.2.1-2, NW2.3.4, NW4.4.7, SD1.1.2-3, SD1.2.3, SD1.3.3, SD2.3.3, SD3.5.2, SD3.5.7, SD4.1.1-4, SD4.2.1, SD4.3.1, SD4.5.1-4, SD4.5.7, SD4.5.9, SD4.6.3-4, SD4.6.6-7, SD5.1.4, SD5.2.5, UE3.4.1, UE3.4.6

Desktop application
CI1.3.2, UE1.2.5, UE1.2.7, UE3.4.1, UE3.4.2, UE3.4.3, UE3.4.4, UE3.4.6, UE3.4.7

Inventory
UE3.1

Development

Environment(s)
CI2.1.3, **SD1.4**, SD1.4.1-4, SD2.3.3, SD2.3.5, SD5.2.1

Life cycle
SD1.2.1, SD1.2.7, SD1.3.1, SD1.3.3

Management
SD2.3.3

Methodology(ies)
SD1.2, SD1.3.1, SD2.3.3, UE3.4.1-2

Process
SD1.3.3-4, SD1.4.4, SD2.3.1-2, SD2.3.4, SD3.5.2

Risks
SD1.3.2, SD3.5.1, SD3.5.4, SD3.5.7

System(s),
SM2.3.2, SM2.5.3, SM3.1.5, SM3.3.1-2, SM4.1.4, SM7.1.1, CI3.5.2, SD4.5.9

Diagnostic

Ports
NW3.7.2

Tools
NW2.3.5

Dial-up connections
CB4.3.4, NW1.5.2, NW2.3.6

Digital

Certificate(s)
SM5.2.8, SM6.1.1, SM6.2.1, CB6.3.1, UE5.2.6, UE5.3.6

Rights Management
SM2.2.4

Signature(s)
SM2.2.4, SM3.1.6, SM6.1.1, SM6.2.2, SM6.3.5, CB2.6.1, CB5.2.3, CB6.1.3, CB6.3.2, CI5.3.3, NW4.3.3, SD4.3.3-4, UE1.5.3, UE5.1.3, UE5.2.6, UE5.3.6

Disaster(s)
SM6.2.4, SM6.7.8, CB2.5.5, CB4.4.4, CB6.3.4, CI3.2.6, CI6.1.3, CI6.1.6, CI6.2.1, NW3.5.4, UE6.3.5, UE6.5.6

Natural,
SM4.7.4, CB2.5.6, CI2.6.1, CI6.2.2, UE6.5.7

Disclosure
SM1.2.7, SM4.2.5, SM6.4.5, CB1.1.1-4, CB2.2.5, CB3.1.4, CB3.4.4, CB6.2.1, CB6.4.5, CI3.2.7, CI4.5.2, CI5.2.4, NW2.2.2, NW2.2.8, NW4.2.4, SD2.2.2, SD2.2.4, SD3.2.2-5, SD4.2.3, SD4.6.8, SD4.6.10, UE1.2.6, UE2.1.2

Non-
SM1.3.2-3, CB6.1.4, CI1.1.3, NW1.1.3, UE1.1.6, UE1.1.9

Unauthorised,
CB2.6.2, CI4.2.3, UE1.2.6, UE6.4.4

DMZ
See Demilitarised Zone (DMZ)

Domain
SM4.1.7, CB2.1.3, NW1.2.2, NW2.3.3

Name(s)
SM6.6.7

E

EAP-TLS
NW2.4.5

Electronic commerce
SM6.6, SM2.2.2, SM2.2.4, SM3.5.2

E-mail(s)
SM6.3, SM1.2.7, SM3.1.2, SM3.1.6, SM5.1.2-3, SM5.2.5, SM5.3.6, SM5.5.3, SM7.2.2, CB3.1.4, CB3.4.4, CB5.2.3, CB6.4.2, CI4.5.4, CI5.2.4, CI5.3.3, NW4.2.4, NW4.3.3, SD2.2.4, SD4.3.3, SD4.6.3, **UE5.2**, UE1.2.5-6, UE1.5.3, UE2.1.2, UE5.1.1, UE5.1.3

Attachments
SM5.1.3, SM6.3.4, SM6.3.7, UE5.1.1, UE5.2.4

Monitoring
SM6.3.6, UE5.2.2-3

Emergency
SM4.7.1-2, SM5.4.4-5, SM6.4.5, CB2.5.3, CB2.5.5, CI2.5.2, CI6.1.2, UE6.5.3, UE6.5.6

Access
CI3.5.2, CI3.5.4-5

Bypass
NW5.2.2

Conditions
CB2.1.4, CI1.1.2, NW1.1.2, SD1.1.3, UE1.1.4

Equipment
CI2.6.4, CI2.7.2-3

Fixes
CB2.3.1, **CI3.5**, CI3.3.1, NW3.2.1, UE2.3.2, UE2.3.7-9

Procedures
SM4.7.2, SM5.1.4, SM5.2.7, CI2.6.4, CI2.8.3, CI6.1.5

Response
SM5.4

Response process
SM5.4.1-2

Response team
SM5.3.10, SM5.4.1-2

Situation
SM4.5.5, SM5.4.3, UE6.4.6

Encryption

SM3.4.7, SM3.5.2, SM6.1.1-2, SM6.3.1, SM6.3.5, SM6.3.7, SM6.4.1, SM6.4.3-5, SM6.5.3, SM6.8.2, CB3.1.4, CB3.3.1, CB3.3.3, CB4.4.2, CB5.3.6, CB6.4.5, CI1.2.3, CI2.2.2, CI2.4.1, CI2.4.3, CI3.2.7, CI5.4.7, NW1.2.2, NW1.5.3, NW2.1.4, NW2.4.2, NW2.4.6, NW3.5.2, NW4.4.7, NW5.4.1, NW5,4.3, SD3.5.7, SD4.1.1, SD4.3.3, SD4.6.8, UE1.3.2-3, UE2.1.2, UE4.1.2, UE4.2.2-3, UE4.3.2-3, UE5.1.3, UE5.2.4, UE5.2.6, UE5.3.4, UE5.3.6, UE5.6.4, UE6.4.4

Environmental

Controls

CB3.3.2, CI2.4.2, UE4.1.1

Control equipment

SM4.7.4, CI6.2.2

Hazards

CI2.6.4

Protection

UE6.4.1

Services

SD5.1.3

Error / exception

CB2.1.3, CB2.1.4, CB2.1.5, CB2.2.5, CB5.3.3, CI1.1.2, CI1.1.3, CI5.4.4, NW1.1.2, NW1.1.3, NW4.4.4, SD1.1.3, SD2.2.3, SD2.2.6, SD3.5.4, SD4.2.3, SD5.1.5, SD5.1.7, UE1.1.3-5, UE3.2.2, UE3.2.4, UE3.2.6, UE3.3.4

Error recovery

SD6.1.3

Escalation

SM4.6.4, SM5.3.10

Event log

SM4.6.6, SM5.2.6, CB2.2.6-7, CB2.4.5, CB3.1.6-7, CI1.4.1, CI2.2.2, CI2.2.7-9, CI3.4.5, NW2.1.2, NW3.3.5, NW5.4.1, SD4.2.3, UE6.2.4

Event logging

CB6.3.3, CI2.2.1-2, CI2.2.4-6, NW2.3.7, SD4.6.3

Evidence

SM4.3.8, SM5.5.3

Admissible,

SM5.5.2

Analysis of,

SM5.5.4

Collection of,

SM5.5.3-4

Handling of,

SM4.6.7, CB2.4.5, CI3.4.5, NW3.3.5, UE6.2.4

Log of recovered,

SM5.5.2

Preservation of,

SM5.5.2, SM5.5.4

Tampering with,

SM1.2.7, SM5.5.4, CB3.4.4, CI5.2.4, NW4.2.4, SD2.2.4, UE1.2.6

Executable

SM6.4.7

Code,

SM5.1.1, CB3.3.1, CB3.3.3, CB3.3.5, CI1.2.3, CI2.4.1, CI2.4.3, CI2.4.5, SD1.4.3, SD6.2.2

File

SM5.2.5

Server-side,

SD4.6.10-11

Software

CI2.1.4

External

Access

CB4.3.3-5, **NW2.3**, **NW2.3**

Assessment

SM4.3.3, SM7.2.2, CI2.5.4, SD4.4.4

Audit

SM7.2.2

Connections

CB4.3, NW2.3.1-8, SD2.2.4

Expertise

SM2.3.3, SM4.1.3, CB5.1.2, CI5.1.2, NW4.1.2, SD2.1.2, UE1.4.3

Hard disk drive

See Portable storage media

Individuals

SM1.2.4, SM1.3.3, SM1.3.5, SM1.3.7, SM2.4.2, SM3.3.2, SM4.6.5, CI1.1.3, NW1.1.3-4, NW2.3.3, NW3.4.1, NW3.7.1, UE1.1.9, UE1.2.1, UE4.2.3, UE4.3.2

Locations

SM3.3.2, CB4.5.5, CI4.5.5

Networks

NW1.3.4, NW2.2.1

Parties

SM5.1.4, SM6.1.2, SM7.2.4, CB2.2.3, NW1.4.2, NW2.3.4

Service providers

CB4.1.1, CB4.1.2, CI1.2.1, NW1.3.2, NW1.4.2, NW1.5.1, NW5.4.1, SD6.1.2

F

Fall-back

SM4.7.2, CI6.1.5, NW1.3.2, NW5.2.2, SD3.1.4, SD4.3.5, SD5.1.5, SD5.2.4, SD6.1.2, SD6.2.2

Fault tolerant

CB4.2.3, CI2.1.2, CI2.5.2

Federal Information Processing Standards (FIPS)
SM4.3.3, CI2.5.4, SD4.4.4

File Transfer Protocol (FTP)
CB2.2.6, CB6.4.6, CI2.3.2, NW2.2.3-5, SD4.6.7

FIPS
See Federal Information Processing Standards (FIPS)

Fire alarms
CI2.6.3, CI2.8.7, UE6.4.7

Fireproof safe(s)
CB2.6.2, CB4.4.4, CI3.1.5, CI3.2.6, NW3.5.4, UE6.3.5, UE6.4.4

Firewall(s)
SM6.4.7, SM6.5.3-4, SM6.8.3, CB2.5.3, CB2.5.7, CB4.2.3, CB4.3.4, CB4.3.5, CB6.4.2-3, **NW2.2**, NW1.2.2, NW1.3.2, NW1.3.5, NW2.1.1, NW2.3.3, NW2.4.4, NW3.4.1, NW5.4.1-2, SD1.4.2, SD4.6.3-4, UE6.5.3

Application proxy,
CB4.3.4, CB6.4.3, NW2.2.3, SD4.6.4

Log
SM7.2.2

Personal,
SM6.4.7, CB3.3.5, CI24.5, UE5.4.3-4

FireWire
UE4.3.1

Forensic investigations
SM5.5, SM1.2.7, SM2.2.5, SM2.3.3, SM2.5.4, SM4.6.2, SM4.6.4, SM4.6.7, SM5.5.1, SM5.5.2, SM5.5.4, SM5.5.5, CB2.4.7, CB3.4.4, CB5.1.2, CI2.2.2, CI2.2.9, CI3.4.7, CI5.1.2, CI5.2.4, NW3.3.7, NW4.1.2, NW4.2.4, SD2.1.2, SD2.2.4, UE1.2.6, UE1.4.3, UE6.2.6

Fraud
SM3.4.4, SM7.2.2, SM7.2.6, CB2.1.5, CB2.4.7, CB5.3.3, CI1.1.3, CI3.4.7, CI5.4.4, NW1.1.3, NW3.3.7, NW4.4.4, NW5.3.4, SD3.2.2, SD3.3.2, SD3.4.2, SD3.5.4, UE1.1.5, UE6.2.6

FTP
See File Transfer Protocol (FTP)

G

Gateway(s)
SM5.2.2, SM6.8.2, NW2.3.4

General controls
UE5.1

General security controls
NW5.4.1, NW5.4.2, **SD4.3**, SD2.3.3

Google Talk (VoIP Service)
SM6.8.1, UE5.3.2, UE5.5.2

Government
SM2.2.5

H

Hand-held devices
UE4.2

Handling information
See Sensitive information

Hardware
SM3.4.7, SM4.1.7, SM4.3.1-4, SM4.3.6-7, SM5.3.5, SM7.2.6, CB4.2.1, CB4.2.3, CB5.3.6, CI1.2.3, CI1.3.1-3, CI2.5.2-4, CI3.3.1, CI3.5.2, CI5.4.7, NW2.4.2, NW4.4.7, SD3.5.7, SD4.4.1-4, SD4.4.6, SD5.1.2-3, SD6.1.4, UE6.5.7

Authentication,
SM1.3.7

Hash / Hash function
SM6.1.1, SM6.3.1, CB2.2.1-2, CI3.2.5, SD4.2.2, UE3.2.3, UE3.3.3

Hazard protection
CI2.6, NW3.4.2, UE6.4.7

High-level

Committee
SM2.4.1, SM4.2.1-2, SM6.6.2, SM7.2.4

Control
SM2.1

Privileges
CB3.1.8, CB6.4.2, CB6.4.4, CI4.3.4, SD4.1.2, SD4.6.3, SD4.6.5

Working group
SM2.1.2-4, SM2.4.1, SM4.1.5

Health Insurance Portability and Accounting Act (HIPAA)
SM4.2.6, SM3.5.2, UE6.1.4

Host intrusion detection systems (HIDS)
SM5.3.4, UE5.4.4

Host system configuration
CB2.2.5-6, **CI2.3**, CI2.3.1-4, UE5.4.4

HTTP
NW2.2.8, SD4.6.8, SD4.6.10

Human rights
SM3.5.2, SM5.5.3

Hyperlink
SM5.1.3, CB6.4.6, SD4.6.7, SD5.1.5

I

Identification labels
SM6.4.6, CB3.3.4, CI2.4.4, CI2.8.6, NW1.4.4, UE4.1.3

Identity and Access Management (IAM)
SM4.4

IEEE 802.1X
NW2.4.5

Illegal material

SM1.2.7, CB3.4.4, CI5.2.4, NW4.2.4, SD2.2.4, UE1.2.6

Incident management process

SM4.6.6-7, SM5.3.2, CB2.4.1-7, CI3.4.1-7, NW3.3.1-6, UE6.2.1

Incident(s)

Business impact of,

SM4.6.4, SM5.3.8, CB2.4.4, CI3.4.4, NW3.3.4, UE6.2.3

Financial impact of,

SM7.2.6

Handling procedures

SM6.5.2

Information security,

SM1.2.7, SM2.1.4, SM2.2.2, SM2.4.1, SM2.4.3-4, SM3.4.4, SM3.4.7, SM4.6.1-7, SM5.1.4, SM5.2.7, SM5.5.1-3, SM6.7.4, SM7.2.2, SM7.2.6, CB2.4.2-7, CB3.4.4, CB5.3.3, CB5.3.6, CB6.1.2-3, CI2.2.2, CI2.2.4, CI3.4.2-7, CI4.1.4, CI5.2.4, CI5.4.4, CI5.4.7, NW3.3.2-7, NW4.2.4, NW4.4.4, NW4.4.7, SD2.2.4, SD3.5.4, SD3.5.7, SD6.3.2, UE1.2.6, UE6.2.1-6

Management

SM2.2.2, SM4.6.3-4, SM6.7.5, CB4.1.3, CI1.2.3, NW1.5.3, NW3.1.4

Management process

SM4.6.6-7, SM5.3.2, CB2.4.1-6, CI3.4.1-7, NW3.3.1-6, UE6.2.1

Team

SM4.6.4, CB2.4.5, CI2.2.8, CI3.4.5, NW3.3.5, UE6.2.4

Independent

Assessment / review

SM4.3.7, SM5.5.4, CB5.4.1, CB5.4.4, CB6.4.1, CI1.3.4, CI5.5.1, CI5.5.4, NW3.7.1, SD2.3.4, SD4.6.2, SD5.2.3

Audit / review

SM7.1.1-2, CB4.1.6, CB5.4.1, CB5.4.4, CI5.5.1, CI5.5.4, NW4.5.1, NW4.5.4, SD2.3.1, UE3.4.7

Confirmation

SM4.1.7, CB3.1.4, CI4.5.4, NW1.5.6

Expert / specialist

SM5.5.4, SM4.1.3, UE3.4.7

Testing

SD5.2.1

Third party

SM5.5.4, SM7.1.2, CB5.4.4, CI5.5.4, NW4.5.4, SD2.3.4

Information classification

SM3.1, **CB5.2**, **CI5.3**, **NW4.3**, **UE1.5**

Details

SM3.1.7-8, SM4.6.2, CB5.2.5-6, CI5.3.5-6, NW4.3.5-6, UE1.5.5

Labelling

SM3.1.6, CB5.2.6, CI3.1.4, CI5.3.6

Requirements

SM3.4.5, CB5.2.4, CB5.3.4, CI4.1.2, CI5.3.4, NW4.3.4, NW4.3.6, NW4.4.5, SD3.5.5

Scheme

SM3.1.1-5, CB5.2.1-3, CI5.3.1-3, NW4.3.1-3, SD3.1.4, UE1.5.1-3, UE3.4.2

Information interchange agreements

SM3.2.2

Information privacy

SM4.2, **UE6.1**

Information risk

SM4.1.4, SM7.2.3, SM7.2.7, UE1.2.5, UE5.5.3

Analysis(es)

SM1.2.3, SM1.2.5, SM2.2.2-3, SM2.4.1, SM2.5.4, SM3.3.1-4, SM3.4.6, SM3.4.8, SM3.5.3, SM4.7.1, SM6.6.3, SM6.7.2, CB5.3.1-8, CI5.4.1-9, NW2.4.1, NW4.4.1-9, SD1.1.2, SD1.3.2, SD2.3.3, SD3.5.1-8, UE3.4.4-5

Analysis methodology(ies)

SM2.2.5, SM2.3.3, **SM3.4**, SM6.6.3, CB5.1.2, CB5.3.1, CI5.1.2, CI5.4.1, NW4.1.2, NW4.4.1, SD2.1.2, SD3.5.1, SD3.5.3, UE1.4.3, UE3.4.4

Practitioner

SM3.3.3, CB5.3.2, CI5.4.3, NW4.4.3

Information Risk Analysis

CB5.3, **CI5.4**, **NW4.4**, **SD3.5**

Managing,

SM3.3

Information Risk Analysis Methodology

SM3.4, SM6.6.3, CB5.3.1, CI5.4.1, NW4.4.1, SD3.5.1, UE3.4.4

Information security

Arrangements

SM2.2.2, SM7.1.1, SM7.2.5, CB2.5.3, CB2.5.7, CB5.1.1-2, CB5.4.3, CB6.1.3, CI5.1.1, CI5.5.3, NW4.1.1, NW4.5.3, SD2.1.1, SD2.3.3, UE1.4.1, UE6.5.3

Effectiveness of,

SM2.2.2, SM7.2.5

Function

SM2.2, SM2.3.4, SM3.5.5, SM6.5.6, SM6.6.2, CB5.1.2, CI5.1.2, NW4.1.2, SD1.2.4, SD2.1.2, SD2.2.3, UE1.4.3

Head of,

SM2.1.3, SM2.2.1, SM2.3.4, SM3.5.1

Managers

SM4.1.5

Policy(ies)

SM1.2, SM1.1.4, SM2.1.4, SM2.4.3, SM7.2.8, CB3.4.1, CB3.4.3, CB6.1.1, CI4.1.2, CI5.2.1, CI5.2.3, NW1.1.4, NW2.2.6, NW4.2.1, NW4.2.3, SD1.2.2, SD2.2.1, SD2.2.3, SD3.1.5, UE1.2.1, UE1.2.3

Practices

SM6.6.4, SM6.7.2, CB6.1.1

Practitioner
CB5.3.2, CI5.4.3, NW4.4.3, SD3.5.3

Principles
SM1.2.2, SM6.5.4, CB2.1.4, CB4.1.2, NW2.2.6, SD4.1.4, UE1.1.4

Responsibilities
SM1.3.1-2, SM2.1.1, SM2.3.1, SM2.4.1, SM3.2.3, CB3.4.2-3, CB5.1.1, CI5.1.1, CI5.2.2, NW1.1.1, NW4.1.1-2, NW4.2.2-3, SD1.1.2, SD2.1.1, SD2.2.3, UE1.1.6

Requirements
SM2.2.3, SM2.5.1, SM3.2.2, SM4.1.2, SM4.1.7, SM4.3.2, SM6.4.1, SM6.6.5, CB5.1.2, CB5.4.2, CI2.5.3, CI2.8.3, CI5.1.2, CI5.5.2, NW1.2.2, NW4.1.2, NW4.5.2, SD1.3.2, SD1.3.4, SD2.3.2, SD4.1.1, SD4.1.3-4, SD4.4.3, SD5.1.2, SD6.3.2, UE1.4.3, UE3.4.2-3, UE3.4.8

Specialist(s)
SM1.3.6, SM2.5.4, SM3.3.3, SM4.1.3, SM6.5.6, SM6.6.6, CB2.4.4, CB2.5.2, CB2.5.6, CB5.3.2, CI3.4.4, CI5.4.3, CI5.5.1, NW3.3.4, NW4.4.3, NW4.5.1, SD2.3.1, SD3.1.7, SD3.5.3, SD4.1.4, UE6.2.3, SD6.3.3, UE6.5.8

Status
SM2.1.4, SM7.2.3, CB5.1.3, CB5.4.3, CI5.1.3, CI5.5.3, NW4.1.3, NW4.5.3, SD2.1.3, SD2.3.3, UE1.4.4

Information security incident management
SM4.6, **CB2.4**, **CI3.4**, **NW3.3**, **UE6.2**,
See also Information security incidents

Installation design
CI2.1.1-2

Installation owner(s)
CI1.1.1, CI1.4.8, CI3.5.5, CI4.1.2, CI4.2.2, CI4.4.5, CI5.1.1, CI5.1.3, CI5.4.3, CI5.4.8, CI5.5.4-6, NW3.1.7

Installation process
SD6.2, SD2.3.3

Instant messaging
SM6.8, SM1.2.7, SM3.1.2, SM3.3.2, CB3.4.4, CI5.2.4, NW4.2.4, NW4.3.3, SD2.2.4, **UE5.3**, UE1.2.6, UE1.5.3, UE5.1.1, UE5.1.3

Application
SM6.8.2-3

Infrastructure
SM6.8.3

Monitoring
SM6.8.1, **UE5.3**

Ports
SM6.8.2-3

Server(s)
SM6.8.3

Services
SM6.8.1

Software
SM6.8.2

Traffic
SM6.8.2-3

Insurance
SM2.1.3, SM3.5.1, SD3.2.2, SD3.3.2, SD3.4.2

Integrity
SM1.2.3, SM2.4.3, SM3.1.1, SM3.4.4, SM4.4.5, SM4.6.1, SM6.1.2, SM6.3.6, SM6.7.4, CB2.2.3, CB3.4.3, CB5.2.1, CB5.3.3, CB6.1.4, CB6.2.1, CI1.2.3, CI1.4.5, CI5.2.3, CI5.3.1, CI5.4.4, NW4.2.3, NW4.3.1, NW4.4.4, SD1.3.2, SD2.2.3, SD2.3.3, SD3.1.3, SD3.3.1, SD3.5.4, SD4.1.1, SD4.1.3, SD4.2.1-2, SD4.3.1, SD4.3.4, UE1.2.3, UE1.5.1, UE3.2.3, UE3.2.6, UE3.3.3, UE3.3.5, UE3.4.2, UE3.4.9, UE5.2.6, UE5.3.6

Requirements
CB1.2, **SD3.3**

Intellectual property rights
SM3.5.2, SM6.7.7, CB6.1.3

Internal audit
SM2.1.3, SM3.5.1, CB5.4.1, CI5.5.1, NW4.5.1, SD2.3.1

Internet
SM1.2.7, SM3.4.4, SM5.2.2, SM5.2.5, SM5.5.3, SM6.1.2, SM6.4.7, CB3.3.5, CB3.4.4, CB5.3.3, CB6.4.2, CI2.4.5, CI5.2.4, CI5.4.4, NW1.5.2, NW4.2.4, NW4.4.4, SD2.2.4, SD3.5.4, SD4.6.3, UE1.2.6, UE5.1.1, UE.5.4.1, UE5.4.3-4, UE5.4.7-8

Access
SD2.2.4, **UE5.4**, UE5.1.1

Café
SM6.4.5

Monitoring
UE5.4.3, UE5.4.5

Service Application Programming Interface (ISAPI)
SD4.6.11

Service providers
SM6.6.7

Intimidation
SM4.5.2, SM4.5.5, UE6.4.6

Intrusion detection / prevention
SM5.3, SM2.2.4, CI2.8.1-2, SD4.4.1

Mechanisms
SM5.3.1, SM5.3.5, CB2.5.3, CB2.5.7, CI1.4.6, UE6.5.3

Methods
SM5.3.2-4

Sensors
SM5.3.5-6, NW1.2.2

Software
SM5.3.7, CI1.4.6, NW3.1.4, UE5.4.4

Inventory(ies)
SM3.1.7, SM4.3.1, SM4.3.6-7, SM5.6.2, SM6.1.4, SM6.5.5, CB4.2.2, CB4.3.2, CB5.2.5, CB6.1.3, CI1.3.1-4, CI2.5.1, CI3.6.2, CI5.3.5, NW1.4.2-3, NW2.3.3, NW4.3.5, NW5.1.3, UE1.5.5, UE3.1.1-4

IP address(es)
CB3.1.6, CB6.4.6, CI2.2.2, CI2.2.5, NW1.2.2, NW2.2.2-3, NW2.2.5, NW4.2.4, SD2.2.4, SD4.6.7

IP Phones
NW5.4.1, NW5.4.3

ISAPI
See Internet Service Application Programming Interface (ISAPI)

ISO/IEC 27002 (17799)
SM2.2.4, CB6.1.2

IT
CI2.1.1, NW1.2.1

Facilities
SM4.5.1, SM4.5.3, SM4.7.5, CB2.4.6, CB4.2.5, CI2.6.2, NW3.3.6, NW5.2.6, UE6.2.5

Function
UE3.1.2, UE6.2.2

Head of,
SM2.1.3

Implementers
SM4.1.3

Infrastructure
SM1.2.4, SM4.1.4, CB6.1.1, NW2.3.3

Management
SM3.5.5, SM6.6.2

Manager(s)
SM2.2.5, SM4.1.5

Planning process
SM2.1.4, CI2.1.1

Projects
SM2.2.3, SM4.1.4

Specialist(s)
SM3.3.3, CB2.3.4, CB2.4.3-4, CB5.3.2, CI3.3.4, CI3.4.3, CI4.1.3, CI5.4.3, NW3.3.3, SD3.5.3, UE2.3.5

Staff
SM2.4.2, SM2.5.3, SM4.4.6, SM4.7.6, CB2.5.6-7, CI6.3.2, UE6.5.8

J

Java
SM5.2.8

Applets
SM5.1.1, SM6.4.1, CB3.3.1, CB3.3.3, CB3.3.5, CI1.2.3, CI2.4.1, CI2.4.3, CI2.4.5, SD1.4.3, UE5.4.8

Script
SM5.1.1, SM5.2.8, SM6.4.1, CB3.3.1, CB3.3.3, CB3.3.5, CI1.2.3, CI2.4.1, CI2.4.3, CI2.4.5, SD1.4.3, SD4.6.10, UE5.4.8

Job description(s)
SM1.3.1, SM1.3.6

K

Key risks
SM3.4.6, CB5.3.5, CI5.4.6, NW4.4.6, SD3.5.6

L

Labelling
SM3.1.6, SM6.3.8, CB5.2.3, CI3.1.4, CI3.2.2, CI3.2.5, CI5.3.3, NW4.3.3, UE1.5.3, UE5.2.5, UE5.3.5

Law enforcement agencies
SM2.2.5, SM4.6.2, SM4.6.5, SM5.4.3

Legal / regulatory

Action
SM5.5.3

Advice
SM5.5.2, SM6.1.4

Bodies
SM5.5.5

Compliance
SM3.5

Function
SM2.1.3, SM3.5.1, SM3.5.5, SM4.6.2, SM4.6.5, SM6.6.2

Liabilities
See Legal Penalties

Non-compliance
SM3.5.3

Obligations
SM1.2.3, SM6.5.2, CI3.2.3, CI4.1.2, NW3.6.3, SD3.1.4, SD3.2.2, SD3.3.2, SD3.4.2

Penalties
SM7.2.2, CB1.1.1, CB1.2.1, CB1.3.1, SD3.2.2, SD3.3.2, SD3.4.2

Responsibilities
SM1.3.2, NW3.6.3, UE1.1.6

Requirements
SM1.2.4, SM3.5.1-2, SM3.5.5-6, SM4.2.3-4, SM4.3.8, SM5.5.4, SM6.4.5, SM6.7.5, SM7.2.7, CB3.1.7, CB6.1.1, CB6.4.7, CI1.4.2, CI2.2.2, CI2.2.4, SD1.2.2, UE6.1.3

Legislation
SM2.2.4, SM3.4.5, SM3.5.2, SM3.5.5, SM4.2.6-7, SM6.5.2, SM6.7.5, CB3.5.4, CI5.4.5, NW4.4.5, SD3.5.5, UE6.1.4

Health Insurance Portability and Accounting Act (HIPAA)
SM4.2.6, UE6.1.4,
See also Health Insurance Portability and Accounting Act (HIPAA)

Sarbanes-Oxley Act
SM1.1.1, SM3.4.7, CB5.3.6, CB6.1.1, CI5.4.7, NW4.4.7, SD3.5.7,
See also Sarbanes-Oxley Act

Liabilities
SM6.5.2, CB1.1.1, CB1.2.1, CB1.3.1, CB6.1.3, SD3.2.2, SD3.3.2, SD3.4.2

Licenses / licensing
SM4.3.1, SM4.3.5, SM6.1.3, SM6.5.2, SM6.7.7, CB6.1.3, CI1.3.1, CI1.3.4-5, SD4.4.2, SD4.4.5

Live environment
SM7.1.3, SM6.6.6, CB2.3.3, CB5.4.5, **CI2.1**, CI3.3.3, CI3.5.2, CI5.5.3, CI5.5.5, NW3.2.3, NW4.5.5, SD1.1.4, SD1.4.2, SD1.4.3, SD2.3.5, SD3.1.4, SD3.1.7, SD5.1.3, SD5.2.1, SD5.2.3, SD5.2.6, SD6.1.1, SD6.1.2, SD6.1.3, SD6.1.4, SD6.2.1, SD6.2.2

Local information security coordination
SM2.3, **CB5.1**, **CI5.1**, **NW4.1**, **SD2.1**, SD2.3.3, **UE1.4**

Local information security co-ordinator(s)
SM2.3.2-3, CB5.1.1-3, CI5.1.1-3, NW4.1.1-3, SD2.1.1-3, UE1.4.1-4

Local security management
NW4.5.3, SD2.3.3

Locks
SM4.5.2-3, SM6.4.2, SM6.4.6, CB3.3.4, CB4.4.4, CI2.4.4, CI2.7.1, CI2.8.1, CI3.1.5, CI3.2.8, NW3.4.2-4, NW3.7.2, UE4.1.3, UE6.3.5, UE6.4.2-4

Logging
SM6.8.2

Access,
SM5.5.3, CB3.1.6, SD1.4.3

Activity
SM6.5.3, SM7.1.3, CB5.4.5, CI1.4.1, CI5.5.5, NW2.1.2, NW2.3.7, NW3.7.1, NW4.5.5, SD2.3.5

Change,
CB2.2.2, SD4.2.3

Configuration
CI2.2.7

Event
SM4.6.2, SM4.6.6, SM5.2.6, CB6.6.3, CI2.2.1, CI2.2.2, CI2.2.4, CI2.2.5, CI2.2.6, NW2.3.7, SD4.2.3, SD4.6.3, UE6.2.2, UE6.2.4

Log-off
SM1.2.6, CI2.3.4

M

Mail server(s)
SM6.3.1-2

Maintenance arrangements / contracts / utilities
SM6.4.1-3, SM7.2.6, CB3.3.1-3, CI2.4.1-3, NW5.2.3, UE4.1.1-2, UE4.2.1

Malicious code
SM6.3.4, CB2.3.3, CI3.3.3

Malicious intent
CI1.1.3, NW1.1.3

Malicious mobile code
SM5.1.1, SM5.2.4, SM6.4.1, CB3.3.1, CB3.3.3, CI1.2.3, CI2.4.1, CI2.4.3, SD1.4.3, UE4.1.2, UE4.2.2

Malware protection

General,
SM5.1

Software
SM5.2

Management commitment
SM1.1

Master files
CB2.1.3, CB2.3.5-6, UE1.1.3, UE2.3.6

Messaging gateways
SM5.2.2, SM6.8.2

Mobile code
SM5.2.8, SM6.4.7, CB3.3.5, CI2.4.5, SD1.4.3, UE5.4.4, UE5.4.8,
See also Malicious mobile code

Monitoring

Audit / review teams
SM7.1.3, CB5.4.5, CI5.5.5, NW4.5.5, SD2.3.5

Electronic communication
SM6.3.6, SM6.6.7, UE5.1.2, UE5.2.2-3, UE5.3.2-3

Information security
SM1.1.3, SM2.1.4, SM2.4.4, SM3.4.7, SM5.1.4, SM5.5.2, SM6.6.7, SM6.8.1, SM7.1.1, SM7.2.1-3, SM7.2.5-8, CB2.1.3, CB5.3.6, CB6.1.3, CI1.4.8, CI5.4.7, NW4.4.7, SD3.5.7, UE1.1.3

Internet
UE5.4.3, UE5.4.5

Network
CI1.4.5, NW1.1.5, NW1.2.2, NW3.1.1, NW3.1.3, NW3.1.5-7

Performance
SM2.1.4, CI1.4.1, CI1.4.4, NW3.1.1

Sensitive material
CB2.6.2, UE6.4.4

Software
CI1.4.1, CI1.4.5, NW3.1.1, UE4.1.2

System(s)
CB2.1.3, CI1.4.2, CI1.4.5, CI2.6.3-4

Telephone
NW5.2.1, NW5.3.3

User
CB6.1.3

Visitors
SM2.8.3

Vulnerabilities
NW1.3.5

VoIP
NW5.4.1-3, UE5.5.2

Wireless
UE5.6.2, UE5.6.4

MP3
UE4.3.1, UE6.2.1

N

Name servers
NW2.3.4

NAT
See Network Address Translation

Network
CB2.3.1

Address Translation
NW2.2.8

Cabling
CB2.5.6, NW1.4.1, NW5.2.5, UE6.5.7

Configuration
NW1.4.1-2, NW2.1.1, NW2.1.5, NW2.4.2, NW3.1.3, NW5.1.2, NW5.3.2

Connections
CB2.4.5, CB4.3.5, CB6.4.2, CI3.4.5, NW1.4.1, NW1.5.2, NW2.3.1, NW2.3.7-8, NW3.3.5, SD3.1.2, SD4.6.3, UE6.2.4

Design
NW1.2, NW2.3.4, NW3.2.5, NW4.2.4

Devices
CI2.2.4, CI2.5.2, CI2.8.4, CI2.8.6, NW1.2.2, NW1.5.3, NW2.1.1-5, NW2.4.2, NW3.1.3, NW3.3.5, NW3.4.4

Documentation
CB4.2.2, **NW1.4**, NW1.1.3, NW2.3.5, NW3.6.2, NW5.1.2

Equipment
CB2.5.6, CB4.2.4, CI6.2.2, NW1.3.2-3, NW1.4.1-2, NW1.4.4, NW2.3.5, NW3.2.1, NW3.4.2, NW3.6.2, NW3.6.4, NW3.7.2, SD4.4.1, UE6.5.7

Gateway
NW2.3.4

Management
NW1.1.1, NW1.2.2, NW2.3.5, NW4.5.3

Monitoring
NW3.1, NW1.1.5, NW1.2.2

Names
NW2.3.4

Owner
NW1.1.1, NW2.2.7, NW2.3.2, NW2.4.1, NW3.1.7, NW3.3.4, NW3.6.3, NW4.1.1, NW4.1.3, NW4.4.3, NW4.4.8, NW4.5.4-6

Services
SM4.7.4, CB4.1.1, CB6.4.2, NW1.3.4, NW1.5.2, NW2.2.3, NW3.6.1-3, NW5.5.2, SD4.6.3

Third party,
CB6.1.1

Time
CI2.2.5

Traffic
SM5.2.2, SM5.2.5, SM5.3.5, CB2.1.3, NW1.3.2, NW1.3.5, NW1.5.3, NW2.1.2, NW2.2.2, NW2.2.4, NW2.2.6, NW2.3.4, NW3.1.4, UE5.6.4

Tools
CI1.4.5, NW1.4.3, NW2.1.4, NW2.3.5, NW3.1.3, NW3.1.5, NW5.4.1-2, SD4.5.4-5

Network intrusion detection systems (NIDS)
SM5.3.4-5,
See also Intrusion Detection

Network owner(s)
NW1.1.1, NW2.2.7, NW2.3.2, NW2.4.1, NW3.1.7, NW3.3.4, NW3.6.3, NW4.1.1, NW4.1.3, NW4.4.3, NW4.4.8, NW4.5.4-6

Non-disclosure
SM1.3.2-3, CB6.1.4, CI1.1.3, NW1.1.3, UE1.1.6, UE1.1.9

Non-repudiation
SM6.1.1, SM6.3.1, SM6.3.5, CB2.6.1, CB6.2.1, SD4.3.4

O

Offensive

Content
SM6.3.1, CB6.4.7

Language
UE5.1.1

Statements
SM1.2.7, SM6.3.4, SM6.8.1, CB3.4.4, CI5.2.4, NW4.2.4, SD2.2.4, UE1.2.6, UE5.2.2, UE5.3.2, UE5.4.3, UE5.5.3

Operating procedure(s)
CI6.2.2, SD6.1.3, UE2.3.2

Operating standards
CB1.1.2, CB1.2.2, CB1.3.2, SD3.2.3, SD3.3.3, SD3.4.3,

Operating system(s)
SM2.2.4, SM5.6.1, SM6.2.3, SM6.4.3, SM6.8.3, CB2.2.6, CB3.3.2, CB6.1.1, CB6.3.3, CB6.4.6, CI2.4.2, CI3.6.1, SD4.4.1, SD4.6.7, SD5.1.5, SD5.2.3, UE4.1.1, UE4.2.2

Outsource / Outsourcing
SM6.7, SM2.2.2, SM2.2.4

Overwriting
CB2.2.2, CI2.2.6, CI3.2.5, SD4.2.3

Owners

SM1.1.2, SM1.2.3, SM3.2.1-4, SM3.3.1, SM3.4.8, SM4.1.5, SM5.6.3, SM7.1.3-4, CB2.1.1, CI3.6.3

Application

SM3.3.1, SM7.1.2-4, CB2.1.1-2, CB2.4.4, CB3.1.5, CB4.1.1-2, CB5.1.1, CB5.1.3, CB5.3.2, CB5.3.7, CB5.4.4, CB5.4.6, CI1.2.1-2, CI1.4.8, CI3.4.4, CI4.1.2, CI4.1.4, NW1.5.1, NW3.3.4, NW4.4.3, SD6.1.2

Business

SM2.1.3, SM3.1.3, SM3.3.1, SM3.3.3, SM3.5.1, SM3.5.5, SM6.5.5, SM6.6.2, SM6.7.2-3, SM7.1.2-4, SM7.2.5, CB5.2.4, CB5.3.2, CI1.2.2, CI2.1.4, CI3.2.3, CI3.5.2, CI4.1.2, CI5.4.3, SD1.1.1, SD2.1.3, SD2.3.5, SD3.1.7, SD3.5.3, SD3.5.8

End user environment

SM3.3.1, SM7.1.2-4, UE1.1.1

Information

SM3.1.8, CB5.2.6, CI5.3.6, NW3.4.6, NW4.3.6, UE1.5.5

Installation

SM3.3.1, SM7.1.2-4, CI1.1.1, CI1.4.8, CI3.5.5, CI4.1.2, CI4.2.2, CI4.4.5, CI5.1.1, CI5.1.3, CI5.4.3, CI5.4.8, NW3.1.7

Key

CB6.2.1

Network

SM3.3.1, SM7.1.2-4, CI5.5.4-6, NW1.1.1, NW2.2.7, NW2.3.2, NW2.4.1, NW3.1.7, NW3.3.4, NW3.6.3, NW4.1.1, NW4.1.3, NW4.4.3, NW4.4.8, NW4.5.4-6

System

SM4.4.6, SM7.2.5

Ownership

SM3.2, SM4.3.5, SM6.5.2, SM6.7.7, CB6.1.3, UE1.2.7, UE4.2.3, UE4.3.2

Proof of,

SM4.3.5, CI1.3.5, SD4.4.5

P

Parameter settings

CB2.2.2, CB2.2.6, CI2.3.1, CI2.3.3-4, CI3.5.2, CI6.2.2, NW2.1.2, NW2.1.5, SD4.6.9, UE2.3.2

Password(s)

SM1.2.7, SM4.4.4, SM5.2.5, SM6.4.4, CB2.2.6, CB3.1.1, CB3.1.4, CB3.1.6, CB3.4.4, CB4.3.3, CB6.3.3, CI2.3.4, CI4.1.4, CI4.2.2, CI4.3.3, CI4.5.1-4, CI5.2.4, NW2.1.2, NW2.1.4, NW3.7.1-2, NW4.2.4, NW5.1.1, NW5.3.1, SD2.2.4, SD4.5.4, UE1.2.6, UE1.3.2-3, UE2.1.1-2, UE3.2.5-6, UE3.3.6, UE3.3.8, UE4.2.2-3, UE.4.3.3, UE5.6.4

PAT

See Port Address Translation

Patch management

SM5.6, **CI3.6**

Payment Card Industry (PCI) Data Security Standard

SM2.2.4, SM3.4.7, SM3.5.2, CB5.3.6, CB6.1.1, CI5.4.7, NW4.4.7, UE6.1.4

PDA

See Personal Digital Assistant (PDA)

Penetration tests

SM7.1.3, CB5.4.5, CI5.5.5, NW4.5.5, SD5.1.5, SD5.2.3-4

Personal firewalls

SM6.4.7, CB3.3.5, CI2.4.5, UE5.4.3-4

Personal Digital Assistants (PDA)

SM5.2.2, CB3.3.4, CI2.4.4, CI2.8.6, UE6.3.1

Personally identifiable information

SM1.2.7, SM4.2.2-6, SM6.7.5, CB3.4.4, CI3.1.3, CI5.2.4, NW4.2.4, SD2.2.4, SD5.2.6, UE1.2.6, UE6.1.1-4

Physical

Access

SM4.5.4, **CI2.8**, CI6.2.2, NW3.4.1, SD1.4.4, UE6.4.2-3, UE6.4.5

Assets

SM4.3.7, CI1.3.4

Controls

SM6.4.2, SM6.4.6, CB3.3.2, CB3.3.4, CB4.4.4, CB5.4.5, CI2.4.2, CI2.4.4, CI3.1.5, NW3.7.2, NW4.5.5, SD2.3.5, UE4.1.1, UE4.1.3, UE6.3.5

Material

SM4.5.4, CB2.6.2

Protection

SM4.5

Security

SM2.1.3, SM3.5.1, **NW3.4**, NW5.2.4, UE6.4.4-5

Physical and environmental protection

UE6.4

Physical security perimeter

CI2.8.7

Port(s)

CB3.1.6, CI2.2.5, NW2.2.3, NW2.2.5, NW2.3.5

Diagnostic

NW3.7.2, NW3.5.1

Instant Messaging

SM6.8.2-3

TCP

NW2.2.2-3

Port Address Translation

NW2.2.8

Portable computers / devices

SM6.4.6, CI3.3.4, CI2.4.4, CI2.8.2, UE4.1.3, UE6.3.1

Portable storage device(s)

SM5.2.5, **UE4.3**, UE6.1.2, UE6.3.1, UE6.4.1

Post-implementation review(s)
SD6.3, SD2.3.3

Power

Cables
CI2.7.1

Loss of,
SM3.4.4, CB2.5.6, CB4.2.5, CB5.3.3, CI2.7.2, CI5.4.4, CI6.2.2, NW3.4.1-2, NW3.6.2, NW3.6.4, NW4.4.4, NW5.2.1-2, SD2.2.3, SD2.2.6, SD3.5.4, UE6.4.8-9, UE6.5.7

Supplies
CB4.2.4-5, **CI2.7**, NW1.3.2, NW3.4.2, NW5.2.1, SD5.1.3, UE6.4.8-9

Power / communications services

Loss of,
CB4.2.4, CI2.7.2, NW3.4.2, NW3.6.4, NW5.2.1-2, UE6.5.7

Privacy
See also Information Privacy

Assessment
SM4.2.3, SM4.2.7

Awareness
SM4.2.3, SM4.2.7

Compliance programme
SM4.2.3, SM4.2.7

Policy
CB6.4.1, SD4.6.2

Project management / manager
SM2.4.1, SD1.1.1

Promotion to live environment
SD2.3.3, SD6.1.1-4, SD6.2.1

Proof of ownership
SM4.3.5, CI1.3.5, SD4.4.5

Protection of databases
UE3.3

Protection of spreadsheets
UE3.2

Proxy server(s)
SM5.2.8, NW2.2.8

Public access

Prohibition of,
CI2.8.5

Public key infrastructure (PKI)
SM6.2, **CB6.3**

Public places / areas
SM1.2.7, SM3.3.2, SM4.5.5, SM6.4.5, CB3.4.5, CI2.7.1, CI5.2.5, NW4.2.5, SD2.2.5, UE1.2.4

Q

Qualifications
SM1.3.5, CI1.1.3, NW1.1.3, UE1.1.8-9

Quality assurance
SM6.7.5, **SD1.3**, SD1.1.2

Quantitative targets
SM7.2.5

R

Redundant Array of Independent Disks (RAID)
CB4.2.3, CI2.5.2

References (personal)
SM1.3.5, CI1.1.3, NW1.1.3, UE1.1.8-9

Regulation(s)
SM2.2.4, SM3.4.5, SM3.5.2-3, SM6.4.5, CB5.3.4, CB5.4.5, NW1.2.2, NW4.4.5, SD3.5.5

Basel II
SM2.2.4, SM3.4.7, CB5.3.6, CB6.1.1, CI5.4.7, NW4.4.7, SD3.5.7

Remote maintenance / support
CB3.3.3, CB6.1.1, CI2.4.3, **NW3.7**, NW1.2.2

Remote working
SM6.4, CB4.3.1

Removable storage media
See Portable storage device(s)

Reputation
CB1.1.3, CB1.2.3, CB1.3.3, SD3.2.4, SD3.3.4, SD3.4.4

Resilience
CB4.2, **CI2.5**, **NW1.3**, **NW5.2**, NW5.4.1-2

Response times
SM6.7.4, CB4.1.2, CI1.2.2, NW5.2.3

Right to audit
SM6.7.7, CB6.1.3

Risk

Acceptable level of,
SM3.4.6, SM7.1.2, CB5.4.4, CB6.1.1, CI5.4.6, CI5.5.4, NW4.4.6, NW4.5.4, SD2.3.4

Appetite
SM7.2.5

Management
SM3.3.4

Residual,
SM3.4.8, SM6.6.5, CB5.3.7, CI5.4.8, NW4.4.8, SD3.5.8

Treatment
SM3.4.8, CB5.3.7, CI5.4.8, NW4.4.8, SD3.5.8

Unacceptable level of,
SM7.2.5

Risk analysis
See Information risk analysis(ies), see also Information Risk Analysis Methodologies

Roles and responsibilities
CB2.1, **CI1.1**, **NW1.1**, **SD1.1**, **UE1.1**
See also Ownership

Run-time code
CI2.1.4

S

Sales
SM7.2.6, CB1.1.1, CB1.2.1, CB1.3.1, SD3.2.2, SD3.3.2, SD3.4.2

Sandbox
SM5.2.8

Sarbanes-Oxley Act
SM1.1.1, SM3.4.7, CB5.3.6, CB6.1.1, CI5.4.7, NW4.4.7, SD3.5.7

SDLC
See Development life cycle

Secure Shell (SSH)
SD4.6.7

Secure Socket Layer (SSL)
CB6.4.5, SD4.3.3, SD4.6.8

Security architecture
SM4.1, SM1.1.4, SM2.2.5, SM2.3.3, SM7.1.1, SM7.2.8, CB5.1.2, CI5.1.2, NW4.1.2, SD2.1.2, SD4.1.1, SD4.1.3-4, UE1.4.3

Security assessment
SD5.2.3, SD6.1.2

Security audit / review
SM7.1, SM2.2.3, SM3.2.2, **CB5.4**, CB6.1.3, **CI5.5**, **NW4.5**, **SD2.3**

Security awareness
SM2.4, SM1.2.3, SM2.2.2, SM3.2.3, SM7.1.1, CB2.1.4, **CB3.4**, CB6.1.3, **CI5.2**, CI3.4.1, CI3.4.3-4, **NW4.2**, SD1.1.3, **SD2.2**, SD2.3.3, **UE1.2**, UE1.1.4

Material
SM2.4.2, CB3.4.2, CI5.2.2, NW4.2.2, SD2.2.2, UE1.2.2

Programmes
SM2.2.2, SM2.4.1, SM7.1.1, CB3.4.2, CI5.2.2, NW4.2.2, SD2.2.2, SD2.2.6, UE1.2.2

Security breaches
SM1.2.3, CB2.1.3, NW2.3.7, UE1.1.3

Security controls
Assessment of,
SD4.2.1-3, SD4.3.1-5

Cost(s) of,
SM2.1.4, SM3.4.7, SM7.2.2, SM7.2.6, CB5.3.6, CI5.4.7, NW4.4.7, SD3.5.7, SD6.3.2

Effectiveness of,
SD5.1.2, SD5.1.5, SD6.3.2

Security criteria
SM4.3.3, CI2.5.4, SD4.4.4

Security education / training
SM2.5, SM2.4.2, SM4.1.3, CB3.4.2, CI5.2.2, NW4.2.2, SD2.2.2, UE1.2.2

Security event logging
CI2.2,
See Event log, see also Event Logging

Security guards
SM4.5.2-3, CI2.8.1, UE6.4.2-3

Security monitoring
SM7.2, SM1.1.3, SM2.1.4, SM2.4.4, SM7.1.1

Security policy
See Information Security Policy

Security-positive
Behaviour
SM2.4.5

Environment
SM1.1.1

Security requirements
SM2.2.3, SM2.5.1, SM3.2.2, SM4.1.2, SM4.1.7, SM4.3.2, SM6.4.1, SM6.6.5, CB5.1.2, CB5.4.2, CI2.5.3, CI2.8.3, CI5.1.2, CI5.5.2, NW1.2.2, NW4.1.2, NW4.5.2, SD1.3.2, SD1.3.4, SD2.3.2, SD4.1.1, SD4.1.3, SD4.1.4, SD4.4.3, SD5.1.2, SD6.3.2, UE1.4.3, UE3.4.2-3, UE3.4.8

Security weaknesses
SM1.2.3, SM4.3.3, CB2.1.3, CI2.5.4, NW4.4.4, NW4.4.7, SD1.1.3, SD4.4.2, SD4.4.4, SD4.5.7, UE1.1.3

Security working group / committee
SM2.1.2-4, SM2.4.1, SM4.1.5, SM4.2.1-3, SM6.6.2, SM7.2.4, CB2.5.1, CI6.1.7, CI6.3.3

Segregation of duties
CB2.1.5, CB4.1.3, CI1.1.3, CI1.2.3, CI4.1.2, NW1.1.3, SD4.3.2, UE1.1.5, UE1.2.7

Sensitive
E-mail
SM6.3.5

Environment
SM6.7.2

Information
SM6.1.1, SM6.5.3, **CB2.6**, CB6.2.1, CB6.4.5, CI2.8.7, CI3.1.3, CI3.1.5, CI3.2.7, CI4.5.5, NW4.4.7, SD1.4.3, SD4.5.8, SD4.6.8, UE4.2.3, UE4.3.2

Material / media
SM1.2.6, SM4.5.4, CB2.6.2, CI2.8.2, CI3.1.3-6, UE6.4.4-5

Messages
SM6.8.2

Traffic
NW1.5.3, NW5.4.1, NW5.4.3

Service agreements
CB4.1, **CI1.2**

Service continuity
NW3.6

Service interruptions
NW1.5.3

Service level agreements (SLAs)
SM2.2.3, SM3.2.2, SM6.5.6, SM6.6.7, CB4.1.1, CI1.2.1, CI5.4.2, NW1.2.1, NW1.5.1, NW3.1.1, NW4.3.5, NW4.4.2, SD1.4.5, SD6.1.2

Service providers
SM2.2.5, SM6.6.7, CB4.1.1-6, CB5.2.5, CI1.2.1, CI1.2.5, CI1.4.7, CI2.2.2, CI2.5.5, CI5.3.5, **NW1.5**, NW1.3.2, NW3.1.6, NW3.2.1, NW4.3.5, NW5.2.2, SD6.1.2

Service requirements
CI1.2.1, CI2.1.1, NW1.2.1

Service Set Identifier (SSID)
NW2.4.3

SessionID
SD4.6.9

'Sign off'
SM1.1.4, SM1.3.6, SM3.1.3, SM3.2.3, SM3.4.8, SM3.5.4, SM6.6.5-6, CB2.3.2, CB2.3.4, CB2.5.2, CB4.1.4, CB4.3.1, CB5.2.4, CB5.3.7, CB6.1.2, CI3.3.2, CI3.3.4, CI5.3.4, CI5.4.8, NW2.2.7, NW2.4.1, NW3.2.2, NW3.2.4, NW4.3.4, NW4.4.8, SD3.1.7, SD3.5.8, SD4.1.4, SD4.5.2, SD4.5.9, SD5.1.2, SD5.1.8, SD6.3.3, UE1.2.7, UE1.5.4, UE2.1.6, UE2.3.5, UE3.1.4, UE3.4.3, UE3.4.5, UE5.2.1, UE5.3.1, UE5.4.1, UE5.5.1, UE5.6.1

Sign-on
SM4.4.1

Application,
UE2.2

Attempts
SM4.4.3, CI4.4.2, UE2.2.2

Mechanisms
CB3.2.2-4, CI4.4.2-4, UE2.2.2-4

Process
SM4.4.4, **CB3.2**, **CI4.4**, UE2.2.1

Reduced,
CI2.1.2

Requirement
CI2.3.4, CI4.3.4

Single point of contact
SM5.1.2, SM6.5.3, CB4.1.5, CB5.1.1, CI1.2.5, CI5.1.1, NW1.5.5, NW4.1.1, SD2.1.1, UE1.4.2

Single points of failure
NW1.2.2, NW1.3.2, SD3.1.4, SD4.3.5

Single sign-on
SM4.4.3

Skype (VoIP Service)
NW5.4.1, UE5.5.2

SLAs
See Service level agreements (SLAs)

'Sniffer'
CI1.4.5, NW3.1.3

Software
SM1.3.7, SM2.2.5, SM2.3.3, SM4.1.7, SM4.3.6, SM4.5.4, SM6.7.4-5, SM6.8.2, CB3.3.2, SD5.1.2, UE5.5.3

Acquisition of,
SM4.3.1-2, SM4.3.4, NW1.3.3, SD4.4.1-3, SD4.4.6

Back-up
SM6.4.3, SM6.4.7, CB3.3.3, CB4.4.1-3, CI2.4.3, CI2.5.3, CI3.2.1, NW3.5.1-2, SD4.3.5, UE1.2.7, UE1.4.2, UE6.3.1-4

Change management of,
CB2.3.1, CB2.3.3, CB2.5.3, CI3.3.1, CI3.5.2, NW3.2.1, NW3.2.5, SD6.2.2, UE2.3.2

Configuration
SM5.2.5-8, SM5.3.6-7, SM6.3.1-2, SM6.4.1, SM6.4.3-4, SM6.4.7, SM6.8.3, CB3.3.1, CB3.3.3, CB4.3.5, CB6.4.2, CI2.4.1, SD4.6.3

Developers
SM4.1.3

Libraries
SM7.1.3, CB5.4.5, CI5.5.5, NW4.5.5, SD2.3.5

Licensing / inventory
SM1.2.3, SM4.3.1, SM4.3.5, SM6.5.2, CB6.1.3, CI1.3.1-5, NW1.4.2, SD4.4.2, SD4.4.5

Malfunctions
SM3.4.4, NW1.3.3, UE6.5.7

Malware protection
SM5.2.1-7, SM6.4.1, SM6.4.3, SM6.4.7, CB2.5.3, CB2.5.7, CB3.3.1, CB3.3.3, CI2.1.2, CI2.4.1, CI2.4.3, SD4.4.1, UE1.2.7, UE4.1.2, UE4.2.2, UE6.3.5

Packages
NW3.5.2, SD4.4.1, SD4.5.2, SD4.5.5-6, SD5.1.3

Provision of,
SM6.4.1, CB3.3.1, CB6.1.4, CI2.1.4, CI2.4.1, CI2.5.5, SD6.2.2

Third party,
SM1.2.7, CB3.4.4, CI5.2.4, NW4.2.4, SD4.5.5-6, SD5.1.5, UE1.2.6

Tools
SM2.2.5, SM2.3.3, SM3.4.2, SM4.6.2, SM4.6.7, SM5.3.4, SM5.3.6-7, SM7.1.2-3, CB2.3.5, CB3.3.3, CB4.2.3, CB4.4.4, CB5.1.2, CB5.2.5, CB5.4.4-5, CB6.1.4, CI1.4.1, CI1.4.5-6, CI2.4.1-3, CI3.3.5, CI3.6.4, CI5.1.2, CI5.3.5, CI5.5.4-5, NW1.3.5, NW1.4.3, NW2.1.4, NW3.1.1, NW3.1.4, NW3.2.5, NW3.6.2, NW4.1.2, NW4.3.5, NW4.5.4-5, SD1.4.3, SD2.1.2, SD2.3.4-5, UE1.4.3, UE2.3.6, UE4.1.1-2, UE4.2.2, UE4.3.3, UE5.4.4, UE6.3.5

Unauthorised,
SM3.4.4, SM5.1.3, SD4.3.4, UE1.2.6

Unauthorised copying of,
SM1.2.7, CB3.4.4, CI1.3.4, CI5.2.4, NW4.2.4, SD2.2.4, UE1.2.6

Updates / fixes
SM5.6.1, SM5.6.4, CB4.2.1, CI2.3.1, CI2.5.4, NW1.3.3, NW3.1.4, UE5.4.4

Vulnerabilities
SM2.2.4, SM4.3.3, SM5.2.8, SM5.6.4, CI2.5.5, CI3.5.2, CI3.6.1

Web browser
SM6.4.7, CB3.3.5, CI2.3.5, CI2.4.5, CI2.5.4, CI2.5.5, SD4.4.2, SD4.4.4, SD5.1.5

Source code
CI2.1.4, CI2.4.5, SD1.4.5, SD4.5.4, SD4.6.10, UE3.3.7

Source routing
NW2.1.2

Special access privileges
CI4.1.2, CI4.1.4, CI4.2.4, CI4.3.4, CI4.5.3, CI4.5.5

Special circumstances
CI4.3.3

Special controls
NW5.3

Specification of requirements
SD3.1

Spoofing
NW2.2.4

SSH
See Secure Shell (SSH)

SSID
See Service Set Identifier (SSID)

SSL
See Secure Socket Layer (SSL)

Staff
SM1.1.3, SM1.2.2-4, SM1.3.1, SM1.3.3, SM1.3.5-7, SM2.2.2, SM2.2.5, SM2.4.1-4, SM2.5.1, SM2.5.3, SM3.2.4, SM4.2.7, SM4.3.4, SM4.4.6, SM4.5.2, SM4.5.5, SM4.6.6, SM4.7.6-7, SM6.4.1-3, SM6.4.5, SM6.5.1, SM6.6.5, SM6.7.5, SM7.2.6, CB2.5.2, CB2.5.4, CB2.5.6-7, CB3.4.2, CB4.1.3, CB4.3.1, CB4.4.4, CB5.3.2, CB5.4.1, CB6.1.1, CI1.1.3-4, CI2.6.4, CI2.8.1, CI3.2.6, CI3.5.2, CI4.1.3, CI4.3.1, CI5.2.1-2, CI5.4.3, CI6.3.2, NW1.1.2-3, NW1.3.5, NW2.1.3, NW3.6.2-3, NW4.2.1-5, NW4.4.3, NW4.5.1, NW5.5.3, SD1.1.4, SD1.2.5-6, SD1.3.1, SD1.3.4, SD1.4.3, SD2.2.1-7, SD2.3.1, SD3.1.6, SD3.2.5, SD3.3.5, SD3.4.5, SD3.5.3, SD4.4.6, SD4.5.2, SD4.5.4, SD5.2.1, UE1.1.7-8, UE1.2.1-2, UE4.2.3, UE4.3.2, UE6.3.5, UE6.4.6, UE6.5.8

Agreements
SM1.3

Duties of,
CI1.1.3, NW1.1.3, SD1.1.4

Morale
CB1.1.4, CB1.2.4, CB1.3.4, SD3.2.5, SD3.3.5, SD3.4.5

Standard of Good Practice (SOGP)
SM2.2.4, CB6.1.2

Standards

Compliance with,
SM5.5.2, SM7.2.7, CB5.3.1, CI5.4.1, NW1.3.3, SD1.1.2, SD2.2.3, SD3.5.1, SD3.5.5, UE5.6.3

COBIT
SM2.2.4

Common Critieria
SM4.3.3, CI2.5.4, SD4.4.4

ISO/IEC 27002 (17799)
SM2.2.4, CB6.1.2

Federal Information Processing Standards (FIPS)
SM4.3.3, CI2.5.4, SD4.4.4

Payment Card Industry (PCI) Data Security Standard
SM2.2.4, SM3.4.7, SM3.5.2, CB5.3.6, CB6.1.1, CI5.4.7, NW4.4.7

Standard of Good Practice (SOGP)
SM2.2.4, CB6.1.2

Stateful inspection firewall
See Firewall

Storage facilities
SM7.1.3, CB4.4.2, CB5.4.5, CI2.5.2, CI5.5.5, NW3.5.2, NW4.5.5, SD2.3.5

Storage media
SM4.5.2, SM4.5.4, SM5.2.5, CB2.6.2, CB3.3.3, CI1.2.3, CI2.2.9, CI2.4.3, CI2.5.5, CI3.1.1-3, CI3.1.5-6, NW2.1.2, UE1.1.3, UE6.4.2, UE6.4.4-5

Suppliers
SM4.2.7, SM4.3.2, SM6.4.2, CB2.2.6, CB3.3.2, CB6.1.1, CI2.3.4, CI2.4.2, CI2.5.3, CI3.5.2, NW2.3.5, NW5.3.1, SD3.2.4, SD3.3.4, SD3.4.4, SD4.2.2, SD4.4.2-6

Suspicious activity
SM5.3.6, CB3.1.7, CI1.4.1, CI1.4.6, NW3.1.4

System

Administrators
SM4.4.6, CB3.1.2, CI3.5.2, CI4.2.3, CI4.3.1, NW1.1.3, SD6.1.3

Availability
CI1.4.4

Build
SD4.5, SD2.3.3, SD4.5.9

Capabilities
CI4.1.4

Capacity
SM6.6.5, SD3.1.2, SD5.1.5

Configuration
CB2.3.5, CI3.3.5, NW3.2.5, SD4.6.10, UE2.3.6

Design
SD2.3.3, **SD4.1**, SD4.2.1, SD4.3.1, SD4.5.2, SD5.1.4

Documentation
SM3.1.2, CB5.2.3, CI4.1.3, CI5.3.3, CI6.2.2, NW4.3.3, SD1.4.4, UE1.5.3

Failure
CB4.2.3, SD3.1.2, SD4.1.2, SD5.2.4, SD6.2.2

Implementation
CB3.3.1, CI2.4.1, SD1.1.2

Information
CI3.5.2, NW3.5.1

Management tools
SM6.4.1, SM6.4.3, CB3.3.1, CB3.3.3, CI2.4.1, CI2.4.3, UE4.1.2

Monitoring
CI1.4

Operation
CI5.5.3

Promotion criteria
SD6.1

Utilities
CB3.1.6, CI2.1.3, CI2.3.1, CI2.3.3

Systems development

Head of,
SD1.1.1, SD2.1.1

Life cycle
See Development life cycle

System software
SM4.7.4, CB2.5.6, CI1.3.2, CI4.1.3, CI6.2.2, SD4.4.1, SD5.1.3, UE5.4.4

T

Technical support
SM5.1.2, SM6.4.5, CI4.1.3, SD3.1.4, SD6.2.2

Telephones
SM1.2.7, SM5.1.2, SM5.3.6, CB2.4.3, CB3.4.4-5, CI3.4.3, CI5.2.4-5, CI6.2.2, NW2.3.8, NW2.4.3, NW3.3.3, NW4.2.4-5, NW5.1.1-3, NW5.2.1-5, NW5.3.1-3, SD2.2.4-5, SD6.2.2, UE1.2.4, UE1.2.6, UE6.2.2

Terms and conditions of employment
SM1.3.1-3, UE1.1.6-7

Testing process
SM5.6.1, SM6.5.1, SM6.6.6, SM7.1.3, CB2.3.2, CB2.5.3, CB5.4.5, CI2.1.3, CI3.3.2, CI3.6.1, CI5.5.5, NW1.3.5, NW3.2.2, NW3.7.1, NW4.5.5, **SD5.1**, SD1.1.2, SD1.2.3, SD1.2.7, SD1.4.2, SD2.2.6, SD2.3.3, SD4.5.8, SD5.2.1-6, SD6.1.2-3, UE2.3.3, UE2.3.9, UE3.4.1, UE3.4.8-9, UE6.5.3, UE6.5.8

Theft
SM2.2.4, SM4.5.2, SM4.5.4, SM6.4.5-6, CB2.1.5, CB2.6.2, CB3.3.4, CI1.1.3, CI2.4.4, CI2.8.2, NW1.1.3, SD3.2.2, SD3.3.2, SD3.4.2, UE1.1.5, UE4.1.3, UE6.4.2, UE6.4.5

Third party

Access
SM6.5, SM3.4.4, CB5.3.3, CB5.4.3, CB6.1.1-3, CI5.4.4, NW4.4.4, SD3.5.4

Agreements
CB6.1

Connections
SM6.5.3-5

Experts
SM6.6.5, CB5.3.2, CB5.4.1, CI5.4.3, CI5.5.1, NW4.4.3, NW4.5.1, SD2.3.1, SD3.5.3

Monitoring
SM6.6.7

Products / software
SM1.2.3, SM1.2.7, SM6.4.3, CB3.4.4, CI2.5.4, CI5.2.4, NW3.1.3, NW4.2.4, SD4.4.5, SD4.5.5-6, SD5.1.5, UE1.2.6

Staff
SM1.3.5

Source code
CI2.1.4, SD1.4.5, SD4.5.4, SD4.6.10, UE3.3.7

Specialist
See Third party experts

Threats
SM1.2.4, SM2.1.4, SM2.2.4, SM3.4.4, SM5.1.4, SM6.6.5, SM7.2.3, CB5.1.2, CB5.3.3, CI4.1.4, CI5.1.2, CI5.4.4, NW4.1.2, NW4.4.4, SD2.2.3, SD2.2.6, SD3.5.4, UE1.4.3, UE5.6.4

Time-out
CB3.3.3, CI2.3.1, CI2.3.4, CI2.4.3

Top-level business manager
SM2.1.1, SM6.6.1

Top management
SM1.1.1-4, SM1.3.6, SM2.1.3, SM2.2.5, SM2.4.1-2, SM3.3.1, SM3.3.4, SM3.4.2, SM3.5.1, SM3.5.4-5, SM4.6.3, SM5.4.2, SM5.5.5, SM6.6.2, SM6.6.6, SM7.1.4, SM7.2.1, SM7.2.4, CB5.3.7, CB5.4.6, CI5.4.8, CI5.5.6, NW4.4.8, NW4.5.6, SD2.3.6, SD3.5.8

Trojan horse
SM5.1.1, SM5.2.2, SM6.4.3, CB2.3.3, CB3.3.3, CI1.2.3, CI2.4.3, CI3.3.3, UE4.1.2, UE4.2.2

U

Unacceptable loss
CI1.2.2, NW3.5.3, SD3.4.6, UE6.5.8

Unauthorised change(s) / modifications
SM4.3.7, CB2.1.5, CB2.2.2, CB2.3.2, CB3.1.7, CI1.1.3, CI1.3.4, CI1.4.5, CI3.3.2, CI4.2.3, NW1.1.3, NW2.1.1, NW2.1.4, NW3.2.2, SD1.4.3, SD4.3.4, SD4.5.3, UE1.1.5, UE2.3.3

Unavailability
CB2.5.6, CI6.2.2, NW3.6.2, UE6.5.7

Uninterruptible Power Supplies (UPS)
CB4.2.4, CI2.7.2-3, NW3.4.2, UE6.4.8

Unique identifier(s)
SM4.4.4, CB3.1.1, CB3.2.1, CI1.3.3, CI4.5.3, UE2.1.1, UE2.2.1

Universal Serial Bus (USB) storage
SM1.2.7, SM4.5.2, SM4.5.4, SM5.2.5, CB3.3.3, CB3.4.4, CI2.4.3, CI2.8.2, CI5.2.4, UE1.1.3, UE4.3.1, UE6.3.1, UE6.4.5

Usage reports
CI1.4.7, NW3.1.6, NW5.2.1

USB storage
See Univeral Serial Bus (USB) storage

User authentication
CI4.5

User authorisation
CI4.2

UserIDs
SM4.4.4-5, CB3.1.1, CB3.2.1, CI2.2.2, CI4.1.4, CI4.2.2, CI4.3.2-3, CI4.4.1, CI4.5.1-3, UE2.1.1, UE2.2.1-2, UE4.3.3

User representatives
SM3.3.3, CB2.5.2, CB2.5.6, CB5.3.2, CI5.4.3, CI6.1.3, NW3.6.3, NW4.4.3, SD3.5.3, SD5.1.4

User requirements
NW1.2.1, NW2.2.6

User training
UE1.3

V

Validation
SM4.4.3, SM4.4.5, SM5.6.4, SM7.1.2, CB2.1.3, CB2.2.1-4, CB3.2.2, CB5.4.4, CB6.4.5-6, CI3.2.2, CI3.6.4, CI4.4.2, CI5.5.4, NW2.2.3, NW4.5.4, SD2.3.4, SD4.1.2, SD4.2.2, SD4.6.6, SD5.1.6, SD6.2.2, UE1.1.3, UE3.2.1, UE3.2.3, UE3.3.1, UE3.3.3

Validation and maintenance
CI6.3

Vendor solutions
SM6.6.4

Version control
CB2.3.5, CI3.3.5, NW3.2.5, SD1.4.3, SD4.5.4, UE2.3.6, UE3.2.5, UE3.3.6, UE3.4.7

Virus protection
See Malware protection

Visitors
CI2.8.3

Voice networks
NW5.1

Access control
NW5.3.1

Alternative facilities
NW5.2.2

Business continuity of,
NW5.2.6

Capacity
NW5.2.1

Controls
NW5.3

Documentation
NW1.4, NW5.1.1-3

Voice over IP (VoIP)
SM2.2.4, SM3.3.2, UE5.5.1, UE5.5.4

Controls
NW5.4.1, NW5.4.3

Devices
NW5.4.1, NW5.4.3

Google Talk
UE5.5.2

Monitoring
NW5.4.1-3, UE5.5.2

Networks
NW5.4, NW5.4.1-3, **UE5.5**

Services
NW5.4.1, UE5.5.2-3

Skype
UE5.5.2

Software
UE5.5.3

Traffic
NW5.4.1-3

VoIP
See Voice over IP (VoIP)

Vulnerabilities
SM1.2.4, SM2.2.4, SM3.4.4, SM5.2.8, SM5.6.4-5, SM6.2.3, SM7.2.3, CB5.1.2, CB5.3.3, CB6.1.1, CB6.3.3, CB6.4.6, CI1.4.5, CI2.3.5-6, CI3.6.4-5, CI5.1.2, CI5.4.4, NW1.3.5, NW3.1.3, NW4.1.2, NW4.4.4, NW5.4.1, NW5.4.3, SD1.3.4, SD3.5.4, SD4.5.7-8, SD4.6.7, SD5.1.2, SD5.1.5, SD5.2.3, UE1.4.3

W

WAP
See Wireless Access Protocol (WAP)

Web

Browsers
SM5.2.8, SM6.4.1, SM6.4.7, CB2.2.6, CB3.3.1, CB3.3.5, CI2.3.2, CI2.4.1, CI2.4.5, SD4.6.10, SD5.1.5, UE5.4.2, UE5.4.4-7

Server
SM5.2.2, CB6.4.2-4, CB6.4.6, SD4.6.3-5, SD4.6.7, SD4.6.10

Site(s)
SM2.2.4, SM5.2.8, SM6.3.5, SM6.4.7, SM6.6.7, CB3.3.5, CB6.4.1-2, CB6.4.5-7, CI2.3.6, CI2.4.5, NW1.3.5, SD4.6.2-3, SD4.6.7, UE.5.4.8

Web application sessions
SD4.6.9

Web-enabled

Application(s)
CB6.4, **CB6.4**, SD4.6.1

Development
SD4.6, SD2.3.3, **SD4.6**

Tools
SD4.5.4

WEP
See Wired Equivalent Privacy (WEP)

Wi-Fi Protected Access (WPA)
NW2.4.2, NW2.4.6, UE5.6.4

Wi-Fi Protected Access 2 (WPA2)
NW2.4.2, NW2.4.6, UE5.6.4

Wired Equivalent Privacy (WEP)
NW2.4.2, NW2.4.6

Wireless

Access
NW2.4, NW2.4.1-2, NW2.4.4-7, **UE5.6**, UE5.1.1

Access Point
SM2.8.2, CI2.8.2, CI2.8.6, NW2.4.2-3, UE5.6.4, UE6.4.2

Devices
NW2.4.2

Network
SM3.3.2, CI1.4.5, NW2.4.2, NW3.1.3, UE1.2.6, UE5.6.3-4

Unauthorised
CI1.4.5, NW2.4.2, NW2.4.4, NW3.1.3

Wireless Access Protocol (WAP)
SM5.2.2, UE6.3.1

Workstation
SM5.1.2, SM6.4.1, SM6.4.7

Protection
CB3.3, CB3.3.1-5, **CI2.4**, CI2.4.1-5, SD5.1.5, **UE4.1**, UE4.1.1

WPA
See Wi-Fi Protected Access

WPA2
See Wi-Fi Protected Access 2

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

The Information Security Forum and your organisation...

Established in 1989, the Information Security Forum (ISF) is an international, not-for-profit association of over 300 of the world's leading organisations who recognise the importance of protecting their business information.

Risk Management Tools

An unrivalled portfolio of automated risk management tools, which allow Members to:

- Measure the strength of their information security arrangements
- Benchmark their security arrangements against those of other Member organisations
- Determine the extent to which they comply with leading international standards for information security
- Perform comprehensive information risk analysis
- Calculate return on security investment (RoSI)

Solutions

A comprehensive library of:

- Executive summaries
- Implementation guides
- Briefing papers
- Technical checklists
- Quick reference quides
- Workshop reports
- Fully worked methodologies

Knowledge Exchange

Members benefit from global participation in:

- Work groups / workshops on topical issues in information security
- Regional meetings / summits
- Online 'webcasts'
- MX², a Member-only secure extranet
- Special interest groups on common areas of interest

ISF Annual World Congress

The leading international conference for information security professionals. Key features include:

- Exclusive to ISF Members
- Two places fully funded out of Membership
- Access to latest thinking in information security
- High profile keynote speakers
- Presentations from Members
- Opportunity for Members to sponsor

...a great partnership

For further details about the Information Security Forum contact:

Tel: +44 (0)20 7212 3318
Fax: +44 (0)20 7213 4813

E-mail: isfinfo@securityforum.org
Web: www.securityforum.org

INFORMATION SECURITY FORUM
PROTECTING BUSINESS INFORMATION

The Information Security Forum is an independent, not-for-profit association of leading organisations dedicated to clarifying and resolving key issues in information security and developing security solutions that meet the business needs of its Members.

Members of the ISF benefit from sharing information security solutions drawn from the considerable experience within their organisations and developed through an extensive work programme. Members recognise that information security is a key business issue and the ISF provides a mechanism which can ensure that the practices they adopt are on the leading edge of information security developments, while avoiding the significant expenditure that individual development of solutions would incur.

For further information contact:

Information Security Forum

Tel: +44 (0)20 7213 1745
Fax: +44 (0)20 7213 4813
E-mail: isfinfo@securityforum.org
Web: www.securityforum.org

Classification: Public
Reference: ISF 07 05 01 Copyright © 2007 Information Security Forum Limited.
All rights reserved.